



Proposal to Administer a Spectrum Access System

Response to DA 15-1426

GN Docket No. 15-319

Key Bridge LLC

Jesse Caulfield, CEO

1750 Tysons Blvd., Suite 1500
McLean, VA 22102

Phone: +1 (703) 542-4140

<http://keybridgewireless.com>

Document Information

Document Status Public

Version 1.21.0

Date Printed May 13, 2016

Copyright © 2016 Key Bridge LLC. All Rights Reserved

Opening Letter

Key Bridge LLC (fmr Key Bridge Global LLC, dba “Key Bridge”, “Key Bridge Wireless”) is pleased to submit this proposal to administer a Spectrum Access System (SAS) in the 3.5 GHz frequency band.¹ This document responds to the Federal Communications Commission's Wireless Telecommunications Bureau and Office of Engineering and Technology invitation for proposal to operate a Spectrum Access System and to administer spectrum operations in the 3,550 to 3,700 MHz band (3.5 GHz).²

While this proposal makes reference to certain aspects in our *Proposal to Administer a Environmental Sensing Capability*, Key Bridge submits this proposal as an independent offer.

As in previous FCC initiatives Key Bridge has collaborated extensively through several multi-stakeholder groups to help develop a body of industry standards and best practices to enable coexistence in 3.5 GHz.³ We are committed and confident in our (and the community's) ability to develop and to implement transparent, neutral, inter-operable spectrum access and monitoring solutions for the 3.5 GHz band that meets or exceeds all of the Commission's requirements.

The Key Bridge SAS architecture and proposed implementation is a comprehensive, end-to-end solution that completely satisfies or, where dependent upon (possibly incomplete) standards or external factors, will be made to satisfy, all of the FCC's current requirements. Our solution is also flexible enough to accommodate future changes or modifications to those requirements.

Key Bridge affirms that it will comply with all applicable rules and enforcement mechanisms and procedures in the operation of our SAS. Key Bridge also affirms that it will comply with subsequent guidance, clarifications and decisions as may be issued from time-to-time by the Commission concerning operation of a SAS. Key Bridge affirms that the Key Bridge SAS will correctly and faithfully implement section §96.55 of the Commission's rules concerning information gathering and retention. To the extent that Key Bridge may require to employ third party suppliers and/or service providers for any aspect of executing our duties, Key Bridge will notify the Commission of such dependency and take care to ensure compliance is assured.

Key Bridge is happy to provide any additional information the Commission may require to evaluate this proposal.

/s/

Jesse Caulfield, CEO
Key Bridge LLC

1 Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3700 MHz Band, GN Docket No. 12-354, *Report and Order and Second Further Notice of Proposed Rulemaking*, FCC 15-47 adopted April 17, 2015 (*Report and Order*)

2 Public Notice, GN Docket 15-319, *[WTB] and [OET] Establish Procedure and Deadline for ... Applications*, DA 15-1426, Released 12/16/2015, (*Request for Proposal*)

3 See for example the Wireless Innovation Forum, the IEEE, the NITRD Wireless Spectrum Research and Development (WSRD) program, the National Spectrum Consortium, and various other private collaborations.

Dependent Works

This document responds to Federal Communications Commission, Wireless Telecommunications Bureau and Office of Engineering and Technology invitation for proposal to operate a Spectrum Access System and to administer spectrum operations in the 3,550 to 3,700 MHz band as described in the Commissions 3.5 GHz *Report and Order*.

In its Report and Order the Commission invited interested parties to cooperatively develop and fine-tune various technical details of concepts and requirements introduced in its new Part 96 rules. Key Bridge is an active and material participant in several multi-stakeholder groups groups developing necessary aspects of Spectrum Access and Environmental Sensing and whose work is ongoing.⁴ Some sections of this proposal reference or are dependent upon these works and our proposal must itself necessarily lack certain details until these works are completed.

Key Bridge will make best effort to implement relevant standards and recommendations produced by multi-stakeholder groups when those works are complete and available. We will amend or update affected sections of this proposal in future upon request.

Notices

This document is provided for the purpose of evaluating our candidacy to operate a Spectrum Access System as envisioned in Part 96 of the Commission's rules. Many of the systems and methods presented herein are covered by issued or pending patents and other intellectual property rights and privileges.

NO GRANT OR PERMISSION IS PROVIDED OR IMPLIED TO ANY PROTECTED SYSTEM, METHOD, UTILITY, COPYRIGHT, TRADEMARK, ETC. BY ITS DISCLOSURE IN THIS PROPOSAL NOR MAY ANY RIGHT, GRANT OR PERMISSION BE PRESUMED OR ASSERTED AGAINST ANYTHING DISCLOSED HEREIN.

This document is copyright © 2016 Key Bridge LLC, all rights reserved.

⁴ The Wireless Innovation Forum, *Spectrum Sharing Committee* and Institute of Electrical and Electronics Engineers (IEEE) *P.1900.5.2 Method for Modeling Spectrum Consumption*, etc.

Table of Contents

1 Responses to Compliance Requirements.....	9
2 Responses to Proposal Conformance Requirements.....	26
3 Definitions and Abbreviations.....	33
4 Key Bridge Qualifications.....	34
4.1 The Key Bridge Team.....	35
4.2 Business Structure.....	37
4.3 Key Personnel.....	38
4.4 Qualifications to Administer a SAS.....	39
5 Key Bridge SAS High-Level Architecture.....	40
5.1 SAS Information Architecture.....	41
5.2 SAS Infrastructure.....	43
5.3 SAS Node.....	44
5.4 SAS Portal.....	45
6 Key Bridge SAS Concept of Operation.....	47
6.1 A Distributed, Meshed, Peer to Peer Application.....	48
6.2 Implementation Example.....	49
6.3 Message Oriented Communications.....	51
6.3.1 Transaction-based Delivery.....	51
6.3.2 At-least-once Message Delivery.....	51
6.3.3 Exactly-once Delivery	52
6.4 SAS User Access Services.....	53
6.5 Facilitating CBSD Coexistence.....	55
6.5.1 Control Channel Messaging.....	57
6.5.2 Pilot Channel Messaging.....	60
6.6 Protecting Federal Incumbent Users.....	63
6.6.1 Informing Incumbent User.....	65
6.6.2 Non-Informing Incumbent User.....	66
6.7 Protecting Non-Federal Incumbent Users.....	67
6.8 SAS Priority Access User Services.....	68
6.9 Modeling and Computing Spectrum Coexistence.....	69
6.9.1 Modeling Transmitters.....	69
6.9.2 Modeling Receivers.....	70
6.9.3 Modeling Signal Propagation.....	70
6.9.4 Computing Spectrum Coexistence.....	71
6.10 SAS Administration Operations.....	73
6.10.1 Records Verification, Correction and Removal.....	73
6.10.2 Interference Incident Reporting and Resolution.....	75
6.10.3 Geographic Boundary Database.....	76
6.10.4 Coordination across International Borders.....	77
6.10.5 Public Data Exports.....	78

6.10.6	Identifying and Validating Protected Entity Records	79
6.10.7	Verifying Equipment Authorization	80
6.10.8	PAL Protection Areas.....	82
7	Key Bridge SAS Functional Architecture.....	83
7.1	SAS Administration Components.....	84
7.1.1	Two-Way Messaging	84
7.1.2	Logging	85
7.1.3	Command, Control and Configuration	86
7.1.4	Enforcement	87
7.1.5	ETL (Extract-Transform-Load)	89
7.2	SAS Operational Components.....	90
7.2.1	Data Storage	91
7.2.2	Data Processing	91
7.2.3	Coexistence Engine	91
7.2.4	SAS to ESC Peering.....	92
7.3	SAS Access Components.....	94
7.3.1	User Access Service.....	95
7.3.2	SAS to SAS Peering.....	96
8	Key Bridge SAS Security Architecture.....	98
8.1	Database Security.....	101
8.2	Communications Security.....	102
8.3	Software Security.....	104
8.4	Public Key Infrastructure.....	105
8.5	Counter-Party Authentication.....	106
8.6	X.509 Digital Certificates.....	108
8.6.1	Public Key Encryption.....	110
8.6.2	X.509 Digital Signatures.....	111
8.7	Message Protection.....	112
8.7.1	Data Confidentiality	113
8.7.2	Data Origin Authentication	113
8.7.3	Data Integrity.....	114
8.7.4	Transport Layer Security	115
8.7.5	Message Layer Security.....	116
9	Key Bridge SAS Commercialization Strategies.....	117
9.1	Services for General and Priority Access Users.....	118
9.2	Automatic Frequency Planning (AFP).....	119
9.3	Spectrum Mapping and Visualization.....	120
9.4	Managed PKI Service.....	121
9.5	Embedded Device Certificates.....	122
10	Appendix: Femto Access Point Use Case.....	123
10.1	Key Bridge FAP Services.....	125
11	Appendix: SSRF Interference Incident Report.....	126
12	Appendix: Joint Spectrum Interference Resolution.....	131

This page intentionally blank.

Illustration Index

Illustration 1: Summary of Key Bridge capabilities.....	34
Illustration 2: Key Bridge SAS / ESC operations center.....	35
Illustration 3: Representative white space portal users.....	39
Illustration 4: Concept Citizens Broadband Radio Service architecture.....	40
Illustration 5: SAS Administration and Service Delivery components.....	43
Illustration 6: A high-level, notional SAS Node architecture.....	44
Illustration 7: Mock-up example of a SAS Administration Portal.....	45
Illustration 8: SAS to SAS peering enables cooperation and collaboration.....	47
Illustration 9: Common application deployment scenarios.....	48
Illustration 10: SAS Infrastructure is a network of SAS Nodes.....	49
Illustration 11: SAS Nodes are dynamically provisioned for real-world demand.....	50
Illustration 12: Transaction-based message delivery pattern.....	51
Illustration 13: At-least-once, exactly-once message delivery pattern.....	52
Illustration 14: SAS Node spectrum service handling.....	53
Illustration 15: Horizontal and vertical spectrum sharing strategies.....	55
Illustration 16: Cognitive control channel to enhance heterogeneous network coexistence.....	57
Illustration 17: Control channel information may be distributed via a mesh overlay.....	58
Illustration 18: Message exchange system.....	59
Illustration 19: Pilot channel messaging.....	60
Illustration 20: Message publish/subscribe system.....	61
Illustration 21: Incumbent Uses in the U.S. 3.5 GHz band.....	63
Illustration 22: Incumbent protections are indistinguishably accumulative.....	64
Illustration 23: Incumbent registration portal.....	65
Illustration 24: A modeled transmitter emission.....	69
Illustration 25: A modeled receiver sensitivity.....	70
Illustration 26: Modeled signal propagation to match different configurations.....	71
Illustration 27: Assessing compatibility using spectrum consumption models.....	72
Illustration 28: Key Bridge White Space Portal.....	73
Illustration 29: Example Ticket Tracking System.....	74
Illustration 30: Boundary Web Services, part of Key Bridge GIS suite.....	76
Illustration 31: Plot of the U.S. - Mexico Border and territorial seas.....	77
Illustration 32: Key Bridge FCC ULS Database web services portal.....	79
Illustration 33: FCC Equipment Authorization search form and response.....	80
Illustration 34: Automated EAS query.....	81
Illustration 35: SAS Nodes evaluate PAL Protection Area contours in real-time.....	82
Illustration 36: SAS Node administrative components for management and control.....	83
Illustration 37: Example system log contents.....	84
Illustration 38: Example system log contents.....	85
Illustration 39: Example SAS Node interactive console.....	86
Illustration 40: Key Bridge White Space database enforcement portal.....	87

Illustration 41: ETL provides data normalization.....	89
Illustration 42: Operational Components are the core of a SAS Node.....	90
Illustration 43: SAS to ESC Peering masks internal architecture.....	92
Illustration 44: SAS Node access components provide User Access Services.....	94
Illustration 45: SAS to SAS Peering masks internal architecture.....	97
Illustration 46: SAS Infrastructure incorporates layered security domains.....	99
Illustration 47: SAS Node communications are protected by functional security enclaves.....	100
Illustration 48: Authentication using an X.509 certificate.....	105
Illustration 49: Direct authentication uses pre-shared secrets in a trust relationship.....	106
Illustration 50: Brokered authentication decouples the client and service.....	107
Illustration 51: Public key encryption and decryption.....	110
Illustration 52: Creation and verification of a digital signature.....	111
Illustration 53: The process of asymmetric encryption.....	113
Illustration 54: Signing a message with an asymmetric signature.....	114
Illustration 55: Transport layer security is point-to-point.....	115
Illustration 56: Message layer security is end-to-end.....	116
Illustration 57: SIM cards enable secure, assured CBSD operation.....	118
Illustration 58: Spectrum situational awareness is enhanced by empirical measurement.....	120
Illustration 59: Key Bridge SAS Node is a Auto-Configuration Server.....	123
Illustration 60: Key Bridge SAS Nodes support TR-069+196 clients.....	125
Illustration 61: SSRF is an essential technology for many DoD spectrum systems.....	126
Illustration 62: Use Case Diagram for Interference Reporting.....	128
Illustration 63: Interference incident processing history.....	129
Illustration 64: Example interference report message data.....	130
Illustration 65: US&P Terrestrial JSIR Process.....	132
Illustration 66: Space System EMI Resolution Process.....	133
Illustration 67: Operating Clearance business process.....	134
Illustration 68: Operating Clearance activity diagram.....	135

1 Responses to Compliance Requirements

Below we respond, directly and briefly, to the specific requirements identified in the Part 96 rules. Additional context and details are provided in this proposal.

Title 47: Telecommunication

PART 96—CITIZENS BROADBAND RADIO SERVICE

Subpart F—Spectrum Access System

§96.53 Spectrum access system purposes and functionality.

The purposes of the SAS include:

<i>(a) To enact and enforce all policies and procedures developed by the SAS Administrator pursuant to §96.63.</i>	Key Bridge will take care to ensure that the SAS Infrastructure enacts and enforces all applicable policies and procedures.
<i>(b) To determine and provide to CBSDs the permissible channels or frequencies at their location.</i>	Reference Section 7 (Key Bridge SAS Functional Architecture) SAS Infrastructure will provide spectrum availability to CBSDs on a non-discriminatory basis. Reference Section 7.2.3 (Coexistence Engine) CBSD Channels are calculated in the SAS Node <i>Coexistence Engine</i> .
<i>(c) To determine and provide to CBSDs the maximum permissible transmission power level at their location.</i>	Reference Section 7 (Key Bridge SAS Functional Architecture) SAS Infrastructure will calculate and convey to a CBSD the maximum permissible transmission power at its location in furtherance of a stable spectrum operating environment. Reference Section 7.2.3 (Coexistence Engine) CBSD maximum power is calculated in the SAS Node <i>Coexistence Engine</i> .
<i>(d) To register and authenticate the identification information and location of CBSDs.</i>	Reference Section 7.3.1 (User Access Service) SAS Infrastructure will register, authenticate and validate CBSD identification and location information. SAS to CBSD communication is cryptographically

	protected.
<i>(e) To retain information on, and enforce, Exclusion Zones and Protection Zones in accordance with §§96.15 and 96.17.</i>	<p>Reference Section 6.10.3 (Geographic Boundary Database)</p> <p>SAS Infrastructure and SAS Nodes each will retain geographic databases of Exclusion Zones and Protection Zones necessary to implement protection of federal incumbent users and FSS earth stations.</p>
<i>(f) To communicate with the ESC to obtain information about federal Incumbent User transmissions and instruct CBSDs to move to another frequency range or cease transmissions.</i>	<p>Reference Section 7.2.4 (SAS to ESC Peering)</p> <p>SAS Infrastructure will communicate with a ESC via a bilateral, neutral peering relationship to obtain information about the presence or absence of federal Incumbent User spectrum operations.</p> <p>SAS Infrastructure will follow the instructions of the ESC to authorize (or de-authorize) CBSD operations.</p>
<i>(g) To ensure that CBSDs operate in geographic areas and within the maximum power levels required to protect federal Incumbent Users from harmful interference, consistent with the requirements of §§96.15 and 96.21.</i>	<p>Reference Section 7.2.3 (Coexistence Engine)</p> <p>CBSD maximum power is calculated in the SAS Node <i>Coexistence Engine</i>.</p> <p>SAS Infrastructure will authorize CBSD operations only in geographic areas and within power levels necessary to protect federal Incumbent Users from harmful interference in accordance with FCC Rules.</p>
<i>(h) To ensure that CBSDs protect non-federal Incumbent Users from harmful interference, consistent with the requirements of §§96.17 and 96.21.</i>	<p>Reference Section 6.10.3 (Geographic Boundary Database)</p> <p>SAS Infrastructure and SAS Nodes each will retain geographic databases of protection contours for non-federal incumbent users including FSS earth station and grandfathered wireless broadband services.</p> <p>Reference Section 7.2.3 (Coexistence Engine)</p> <p>SAS Infrastructure will implement coexistence policies and authorize CBSD operations to ensure CBSDs protect non-federal Incumbent Users from harmful interference in accordance with FCC Rules.</p>
<i>(i) To protect Priority Access Licensees from interference caused by other PALs and from General</i>	Reference Section 6.10.3 (Geographic Boundary Database)

<i>Authorized Access Users, including the calculation and enforcement of PAL Protection Areas, consistent with §96.25.</i>	<p>SAS Infrastructure and SAS Nodes each will retain geographic databases of priority access licensee regions (i.e. census tracts, claimed areas, etc.).</p> <p>Reference Section 6.10.8 (PAL Protection Areas)</p> <p>PAL Protection Areas will be automatically calculated, persisted and dynamically updated in the SAS Node serving the Priority Access CBSDs and coordinated with other responsible SAS Nodes and external SAS instances via peering.</p> <p>Reference Section 7.2.3 (Coexistence Engine)</p> <p>SAS Infrastructure will implement coexistence policies and authorize CBSD operations to PA users are protected from interference from GA users.</p>
<i>(j) To facilitate coordination between GAA users operating Category B CBSDs, consistent with §96.35.</i>	<p>Reference Section 7.2.3 (Coexistence Engine)</p> <p>SAS Infrastructure will implement coexistence policies and support coexistence strategies that facilitate automated coordination between heterogeneous networks and users GAA CBSDs.</p>
<i>(k) To resolve conflicting uses of the band while maintaining, as much as possible, a stable radio frequency environment.</i>	<p>Reference Section 6.10.2 (Interference Incident Reporting and Resolution)</p> <p>SAS Infrastructure will implement and support manual plus automated methods for interference incident reporting and resolution.</p>
<i>(l) To ensure secure and reliable transmission of information between the SAS and CBSDs.</i>	<p>Reference Section 8.2 (Communications Security)</p> <p>All communications with and within the SAS Infrastructure are cryptographically protected.</p>
<i>(m) To protect Grandfathered Wireless Broadband Licensees consistent with §§90.1307 and 90.1338 of this chapter, and §96.21.</i>	<p>Reference Section 7.2.3 (Coexistence Engine)</p> <p>Grandfathered Wireless Broadband Licensees will be protected in the Coexistence Engine as grandfathered incumbent users consistent with §§90.1307 and 90.1338.</p>
<i>(n) To implement the terms of current and future international agreements as they relate to the Citizens Broadband Radio Service.</i>	<p>Reference Opening Letter.</p> <p>Key Bridge affirms that it will comply with all applicable rules and enforcement mechanisms and procedures in the operation of our SAS. Key Bridge also affirms that it will</p>

	comply with subsequent guidance, clarifications and decisions as may be issued from time-to-time by the Commission concerning operation of a SAS.
<i>(o) To receive reports of interference and requests for additional protection from Incumbent Access users and promptly address interference issues.</i>	<p>Reference Section 6.10.2 (Interference Incident Reporting and Resolution)</p> <p>Interference incident reporting to the SAS Infrastructure will use the <i>SSRF Interference Incident Report</i> (IntfReport) data model, protocol and transaction process defined by the SSRF specification.</p> <p>Interference handling and response procedures will be developed and implemented following guidelines established in the <i>Joint Spectrum Interference Resolution</i> (JSIR) procedures.</p>

§96.55 Information gathering and retention.

<i>(a) The SAS shall maintain current information on registered CBSDs, the geographic locations and configuration of protected FSS locations as set forth in §96.17, and the federal Incumbent User Exclusion Zones and Protection Zones.</i>	<p>Reference Section 7.3.1 (User Access Service)</p> <p>CBSDs must register with the SAS Infrastructure and have established cryptographic credentials prior to communicating with a SAS Node or receiving service.</p> <p>Registered CBSD information is stored in the CBSD's responsible <i>SAS Node</i> database and/or in the <i>SAS Registry Database</i>.</p>
<i>(1) For registered CBSDs, such information shall include all information required by §§96.39 and 96.45.</i>	<p>Reference Section 7.3.1 (User Access Service)</p> <p>A CBSD registration process is under development by a multi-stakeholder group chaired by Key Bridge. This work is in progress.</p> <p>A recently published draft CBSD registration process and messaging format includes all information required by §§96.39 and 96.45 and will be persisted in a <i>SAS Node</i> database or <i>SAS Registry Database</i>.</p>
<i>(2) SAS Administrators must make all information necessary to effectively coordinate operations between and among CBSDs available to other SAS Administrators.</i>	<p>Reference Section 7.3.2 (SAS to SAS Peering)</p> <p>SAS to SAS data exchange necessary to coordinate CBSD and SAS operations is presently under development in a multi-stakeholder group chaired by Key Bridge. This work is in progress.</p>

	A recently published draft SAS peering process and messaging format includes information presently understood to enable coordinated CBSD and SAS operations. This will be further developed, improved and tested in the coming months.
<i>(3) SAS Administrators must make CBSD registration information available to the general public, but they must obfuscate the identities of the licensees providing the information for any public disclosures.</i>	Reference Section 6.10.5 (Public Data Exports) The Key Bridge SAS will make regular snapshot extracts of the <i>SAS Registry Database</i> available for download to the general public. The extracted information will be duly and appropriately obfuscated.
<i>(4) For non-federal Incumbent Users, the SAS shall maintain a record of the location of protected earth stations as well as the all registration information required by §96.17.</i>	Reference Section 6.6.1 (Informing Incumbent User) Location information for existing fixed satellite service stations and grandfathered wireless broadband services will be learned via direct (ETL) data transfer from the FCC. Non-federal incumbent users may supplement FCC licensing information via a <i>SAS Registration Portal</i> as an informing incumbent user.
<i>(b) The SAS shall maintain records not pertaining to federal Incumbent User transmissions for at least 60 months.</i>	Reference Section 5 (Key Bridge SAS High-Level Architecture) Regular snapshots taken from the <i>SAS Registry Database</i> will be cryptographically protected and digitally archived for not less than 60 months using <i>Amazon Glacier</i> , a online solution for non-time sensitive cloud storage offered by our solution partner Amazon Web Services (AWS). Key Bridge will use Amazon Glacier's built-in capabilities to encrypt data at rest using Advanced Encryption Standard (AES) 256-bit symmetric keys in a cloud storage environment designed for eleven 9s of durability (99.999999999%) by synchronously storing data across multiple physical facilities.
<i>(c) The SAS shall only retain records of information or instructions received regarding federal</i>	Reference Section 5 (Key Bridge SAS High-Level Architecture) SAS Nodes are designed to reflect the immediate

<p><i>Incumbent User transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process.</i></p>	<p>instructions and state information presented by a ESC. SAS Nodes are not configured with an ability to retain historical records of information received from the ESC.</p> <p>Centralized SAS systems such as the <i>Administration Portal</i>, the <i>Root Node</i>, a <i>Registry Database</i>, etc. will not have direct access to ESC transmissions. However these centralized systems and applications could potentially learn about ESC spectrum availability information updates during the course of normal operation; they will not be configured to do so.</p> <p>Information retention policies implemented in these centralized systems will comply with whatever constraints are established and conveyed by the ESC. These retention policies and constraints are expected to be either a) fixed: established during the provisioning of a SAS to ESC peering session, or b) dynamic: embedded into the <i>SAS Gateway Protocol</i> used for information exchange between a SAS and ESC.</p>
<p><i>(d) The SAS shall be technically capable of directly interfacing with any necessary FCC database containing information required for the proper operation of an SAS.</i></p>	<p>Reference Section 7.1.5 ETL (Extract-Transform-Load)</p> <p>SAS Infrastructure includes a sophisticated extract-transform-load (ETL) capability to interface and receive information from any necessary FCC database or information resource.</p>
<p><i>(e) The SAS shall process and retain acknowledgements by all entities registering CBSDs that they understand the risk of possible interference from federal Incumbent User radar operations in the band.</i></p>	<p>Reference Section 9 (Key Bridge SAS Commercialization Strategies)</p> <p>Appropriate and necessary user acknowledgements will be duly collected and retained, either directly from GA users during enrollment or indirectly from PA users via their respective service provider.</p>

§96.57 Registration, authentication, and authorization of Citizens Broadband Radio Service Devices.

<p><i>(a) An SAS must register, authenticate, and authorize operations of CBSDs consistent with this part.</i></p>	<p>Reference Section 9 (Key Bridge SAS Commercialization Strategies)</p> <p>All users must register CBSDs with the SAS prior to receiving service from the SAS. The Key Bridge registration process includes establishment and exchange</p>
--	---

	of cryptographic credentials, which are used to positively authenticate and authorize CBSD operations.
<i>(b) CBSDs composed of a network of base and fixed stations may employ a subsystem for aggregating and communicating all required information exchanges between the SAS and CBSDs.</i>	<p>Reference Section 5 (Key Bridge SAS High-Level Architecture)</p> <p>Aggregated operations are natively supported by the Key Bridge architecture. To wit: a <i>SAS Node</i> may be readily configured to operate as a <i>SAS Proxy</i>.</p>
<p><i>(c) An SAS must also verify that the FCC identifier (FCC ID) of any CBSD seeking access to its services is valid prior to authorizing it to begin providing service.</i></p> <p><i>A list of devices with valid FCC IDs and the FCC IDs of those devices is to be obtained from the Commission's Equipment Authorization System.</i></p>	<p>Reference Section 6.10.7 (Verifying Equipment Authorization)</p> <p>Only FCC certified CBSDs will be authorized to communicate with and receive services from they Key Bridge SAS.</p> <p>CBSD credential information, including the FCC identifier plus product type, manufacturer and model, plus user identifying information (i.e. the owner) will be recorded and validated during the CBSD registration process.</p> <p>Reference Section 7.1.5 ETL (Extract-Transform-Load)</p> <p><i>SAS Infrastructure</i> includes a extract-transform-load (ETL) capability to interface and receive device certification information (including certified FCC IDs) from the FCC's Equipment Authorization System.</p>
<i>(d) An SAS must not authorize operation of CBSDs within Protection Zones except as set forth in §96.15.</i>	<p>Reference Section 6.4 (SAS User Access Services)</p> <p>The SAS will conform with procedures set forth in §96.15.</p> <p>CBSD are by default forbidden by the SAS to operate in Exclusion Zones and also by default forbidden by the SAS to operate in Protection Zones.</p> <p>CBSD operation in a Protection Zone is only allowed by the SAS where the absence of NIIU spectrum operations is positively asserted by a ESC.</p> <p>Reference Section 6.10.3(Geographic Boundary Database)</p> <p>NTIA-defined Exclusion Zones and other prescriptive Protection Zone geographic information will be retrieved</p>

	<p>from the <i>Key Bridge Border API</i>.</p> <p>The <i>SAS Infrastructure</i> will retain information on NTIA Exclusion Zones and, when operating with a ESC, ESC-defined Protection Zones in accordance with sections 96.15 and 96.17 of the Commission's rules.</p>
<p><i>(e) An SAS must calculate and enforce PAL Protection Areas consistent with section 96.25 and such calculation and enforcement shall be consistent across all SASs.</i></p>	<p>Reference Section 6.10.8 (PAL Protection Areas)</p> <p>PAL Protection Areas will be automatically calculated, persisted and dynamically updated in the SAS Node serving the Priority Access CBSDs and coordinated with other responsible SAS Nodes and external SAS instances via peering.</p> <p>Development of a standardized model is already under discussion by a multi-stakeholder group in which Key Bridge participates.</p>

§96.59 Frequency assignment.

<p><i>(a) An SAS must determine the available and appropriate channels/frequencies for CBSDs at any given location using the information supplied by CBSDs, including location, the authorization status and operating parameters of other CBSDs in the surrounding area, information communicated by the ESC, other SASs, and such other information necessary to ensure effective operations of CBSDs consistent with this part.</i></p>	<p>Reference Section 6.4 (SAS User Access Services)</p> <p><i>SAS Nodes</i> establish spectrum availability for CBSDs. Spectrum availability calculations incorporate many types of information, which is assembled from a variety of sources; some <i>a priori</i> and some upon demand.</p> <p>Spectrum availability is calculated using the immediately available information to facilitate coexistence and effective operations of CBSDs.</p>
<p><i>All such determinations and assignments shall be made in a non-discriminatory manner, consistent with this part.</i></p>	<p>Reference Section 6.4 (SAS User Access Services)</p> <p>All spectrum availability information will be calculated and provided in a neutral, non-discriminatory manner according to the 3.5 GHz three-tiered spectrum access model.</p>
<p><i>(1) Upon request from the Commission or a CBSD, an SAS must confirm whether frequencies</i></p>	<p>Reference Section 5.4 (SAS Portal)</p> <p>Queries for, and inspection of, frequency availability at</p>

<i>are available in a given geographic area.</i>	<p>any geographic position will be made available through the <i>SAS Community Portal</i>.</p> <p>Queries for, and inspection of, spectrum information across a geographic area is expected to be a premium capability and will be made available to the Commission on request through a special facility.</p>
<i>(2) Upon request from the Commission, an SAS must confirm that CBSDs in a given geographic area and frequency band have been shut down or moved to another available frequency range in response to information received from the ESC.</i>	<p>Reference Section 6.4 (SAS User Access Services)</p> <p>SAS to CBSD communication is managed through <i>User Access Services</i> software modules that implement network-type specific protocols. Each of these protocols will include the capability to positively affirm that CBSDs comply with instructions provided by their responsible SAS.</p> <p>Reference Section 5.4 (SAS Portal)</p> <p>SAS operations and the immediate status of CBSDs under SAS coordination may be directly inspected through the <i>SAS Administration Portal</i>.</p>
<i>(3) If an SAS provides a range of available frequencies or channels to a CBSD, it may require that CBSD to confirm which channel or range of frequencies it will utilize.</i>	<p>Reference Section 6.4 (SAS User Access Services)</p> <p><i>User Access Services</i> supported by <i>SAS Infrastructure</i> will require CBSDs to report their immediate operating channel configuration. Key Bridge does not intend to support User Access Services protocols and formats that do not include this capability.</p>
<p><i>(b) Consistent with the requirements of §96.25, an SAS shall assign geographically contiguous PALs held by the same Priority Access Licensee to the same channels in each geographic area, where feasible.</i></p> <p><i>The SAS shall also assign multiple channels held by the same Priority Access Licensee to contiguous frequencies within the same License Area, where feasible.</i></p>	<p>Reference Section 7.2.3 (Coexistence Engine)</p> <p>The Key Bridge <i>SAS Infrastructure</i> will take care to harmonize, coordinate and stabilize spectrum assignments for PA and GA users. This includes, wherever feasible, assigning the same channel to PA users operating across geographically contiguous census tracts where the license is held by the same network operator and also attempting to maximize the amount of contiguous spectrum in a spectrum assignment.</p>
<i>(c) An SAS may temporarily assign</i>	Reference Section 6.4 (SAS User Access Services)

<i>PALs to different channels (within the frequency range authorized for Priority Access use) to protect Incumbent Access Users or if necessary to perform its required functions.</i>	User Access Services supported by the SAS will enable rapid spectrum clearance and re-allocation of CBSD channels.
--	--

§96.61 Security.

<i>(a) An SAS must employ protocols and procedures to ensure that all communications and interactions between the SAS and CBSDs are accurate and secure and that unauthorized parties cannot access or alter the SAS or the information it sends to a CBSD.</i>	<p>Reference Section 7.3.1 (User Access Service)</p> <p>All SAS to CBSD communications will be cryptographically protected.</p> <p>Key Bridge participates in a multi-stakeholder group that is working to develop a industry standard communications security framework for SAS-to-CBSD communications. This work is also in progress.</p> <p>Reference Section 8.1 (Database Security)</p> <p>Key Bridge implements database security practices to ensure the integrity and confidentiality of system information.</p> <p>Reference Section 8.7 (Message Protection)</p> <p>SAS Infrastructure cryptographically protects message data communications and interactions between the SAS and CBSDs against threats such as eavesdropping and data tampering.</p>
<i>(b) Communications between CBSDs and an SAS, between an ESC and an SAS, between individual CBSDs, and between different SASs, must be secure to prevent corruption or unauthorized interception of data.</i>	<p>Reference Section 8.2 (Communications Security)</p> <p>The SAS employs both transport and message security procedures to protect communications between CBSD, SAS and ESC from data corruption or unauthorized interception.</p> <p>SAS Infrastructure implements a <i>positive security model</i> that does not allow connections or communications with unknown parties. A peered ESC and all CBSDs must be previously registered and have established digital certificates before communications and data exchange with the SAS is allowed.</p>
<i>An SAS must be protected from</i>	Reference Section 8.1 (Database Security)

<i>unauthorized data input or alteration of stored data.</i>	Key Bridge implements database security practices to ensure the integrity and confidentiality of system information.
<i>(c) An SAS must verify that the FCC identification number supplied by a CBSD is for a certified device and must not provide service to an uncertified device.</i>	<p>Reference Section 6.10.7 (Verifying Equipment Authorization)</p> <p>Only certified devices will be authorized to communicate with and receive services from the SAS.</p> <p>CBSD credential information, including the FCC identifier plus product type, manufacturer and model, will be recorded and validated during the CBSD registration process.</p> <p>Reference Section 7.1.5 ETL (Extract-Transform-Load)</p> <p>SAS Infrastructure includes a sophisticated extract-transform-load (ETL) capability to interface and receive device certification information (including certified FCC IDs) from the FCC's Equipment Authorization System.</p>

§96.63 Spectrum access system administrators.

The Commission will designate one or more SAS Administrators to provide nationwide service. The Commission may, at its discretion, permit the functions of an SAS, such as a data repository, registration, and query services, to be divided among multiple entities; however, it shall designate one or more specific entities to be an SAS Administrator responsible for coordinating the overall functioning of an SAS and providing services to operators in the Citizens Broadband Radio Service. Each SAS Administrator designated by the Commission must:

<i>(a) Maintain a regularly updated database that contains the information described in §96.55.</i>	<p>Reference Section 5.2 (SAS Infrastructure)</p> <p>The <i>SAS Registry Database</i> will contain all information described in §96.55 except current information on registered CBSDs, which is contained in the database of each CBSD's respective responsible SAS Node.</p>
<i>(b) Establish a process for acquiring and storing in the database necessary and appropriate information from the Commission's databases, including PAL assignments, and synchronizing the database with the current Commission databases at least once</i>	<p>Reference Section 7.1.5 ETL (Extract-Transform-Load)</p> <p>A <i>Extract-Transform-Load</i> (ETL) process imports external data into the SAS Infrastructure. The imported information may be of any type and format and available anywhere on the Internet.</p>

<i>a day to include newly licensed facilities or any changes to licensed facilities.</i>	
<i>(c) Establish and follow protocols and procedures to ensure compliance with the rules set forth in this part, including the SAS functions set forth in subpart F of this part.</i>	<p>Key Bridge participates in and materially supports multi-stakeholder groups working to establish protocols and procedures to ensure Rules-compliant SAS operation.</p> <p>Key Bridge will take care to implement and follow all applicable and relevant protocols and procedures to ensure compliance with the Rules.</p>
<i>(d) Establish and follow protocols and procedures sufficient to ensure that all communications and interactions between the SAS, ESC, and CBSDs are accurate and secure and that unauthorized parties cannot access or alter the SAS or the information transmitted from the SAS to CBSDs.</i>	<p>Key Bridge participates in and materially supports multi-stakeholder groups working to establish protocols and procedures to ensure secure communications throughout the CBRS ecosystem.</p> <p>Key Bridge will take care to implement and follow all applicable and relevant protocols and procedures to ensure secure, reliable, trusted communications across the entire CBRS ecosystem.</p>
<i>(e) Provide service for a five-year term. This term may be renewed at the Commission's discretion.</i>	Key Bridge intends to provide the services described in this proposal for not less than five years.
<i>(f) Respond in a timely manner to verify, correct or remove, as appropriate, data in the event that the Commission or a party brings a claim of inaccuracies in the SAS to its attention. This requirement applies only to information that the Commission requires to be stored in the SAS.</i>	<p>Reference Section 6.10.1 (Records Verification, Correction and Removal)</p> <p>The <i>SAS Administration Portal</i> will include capabilities to enable the correction or cause the removal of records by authorized administrators. Key Bridge will employ this capability to respond to any notifications from the Commission or other parties of inaccuracies in the SAS. All responses will be made in a timely manner.</p>
<i>(g) Securely transfer the information in the SAS, along with the IP addresses and URLs used to access the system, and a list of registered</i>	Key Bridge will securely transfer SAS operations to another approved entity in the event we do not continue as the SAS Administrator at the end of term.

<i>CBSDs, to another approved entity in the event it does not continue as the SAS Administrator at the end of its term. It may charge a reasonable price for such conveyance.</i>	Any fee for such conveyance will be fair and reasonable.
<i>(h) Cooperate to develop a standardized process for coordinating operations with other SASs, avoiding any conflicting assignments, maximizing shared use of available frequencies, ensuring continuity of service to all registered CBSDs, and providing the data collected pursuant to §96.55.</i>	<p>Reference Section 7.3.2 (SAS to SAS Peering)</p> <p>Key Bridge participates in and materially supports multi-stakeholder groups working to establish standardized process for coordinating operations with and between other SASs.</p> <p>Key Bridge presently chairs one such multi-stakeholder working group.</p>
<i>(i) Coordinate with other SAS Administrators including, to the extent possible, sharing information, facilitating non-interfering use by CBSDs connected to other SASs, maximizing available General Authorized Access frequencies by assigning PALs to similar channels in the same geographic regions, and other functions necessary to ensure that available spectrum is used efficiently consistent with this part.</i>	<p>Reference Section 7.3.2 (SAS to SAS Peering)</p> <p>Capabilities supported by a external SAS peering session include facilitating CBSD service roaming, coordinating operations between and among heterogeneous CBSDs, providing a stable radio frequency environment for users and other functions required for orderly spectrum administration and fulfillment by the SAS of the responsibilities assigned under Part 96.</p>
<i>(j) Provide a means to make non-federal non-proprietary information available to the public in a reasonably accessible fashion in conformity with the rules in this part.</i>	<p>Reference Section 6.10.5 (Public Data Exports)</p> <p>The Key Bridge SAS will make regular snap shot extracts of the <i>SAS Registry Database</i> available for download to the general public.</p> <p>The extracted information will be duly and appropriately obfuscated.</p>
<i>(k) Ensure that the SAS shall be available at all times to immediately respond to requests from authorized Commission personnel for any and all information stored or retained by the SAS.</i>	<p>Reference Section 5.4 (SAS Portal)</p> <p>SAS Infrastructure will operate in a persistent, uninterrupted manner and will be available to provide any information it contains that the Commission may require.</p>

	Key Bridge will provide access through one or more <i>SAS Portals</i> which Commission personnel may use without constraint. Personnel may also contact Key Bridge directly for any information or reports not otherwise available.
<i>(l) Establish and follow protocols to respond to instructions from the President of the United States, or another designated Federal government entity, issued pursuant to 47 U.S.C. 606.</i>	Key Bridge will establish and follow internal procedures to respond in a timely and expeditious manner to instructions from the President of the United States, or another designated Federal government entity.
<i>(m) Establish and follow protocols to comply with enforcement instructions from the Commission.</i>	<p>Reference Section 7.1.4 (Enforcement)</p> <p>SAS Infrastructure includes manual methods plus automated technologies to implement enforcement instructions.</p> <p>Key Bridge affirms our intent to cooperate with enforcement actions and will take care that SAS Infrastructure implement such instructions.</p>
<i>(n) Ensure that the SAS:</i>	--
<i>(1) Operates without any connectivity to any military or other sensitive federal database or system, except as otherwise required by this part; and</i>	<p>SAS Infrastructure does not rely upon nor include connectivity to any military or other sensitive federal database or system.</p> <p>Reference Section 7.1.5 ETL (Extract-Transform-Load)</p> <p>The only federal databases and systems accessed by SAS Infrastructure are those provided by and specifically required by the FCC. These data sources include ULS, IBFS, EAS, etc.</p>
<i>(2) Does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the SAS.</i>	<p>Reference Section 5 (Key Bridge SAS High-Level Architecture)</p> <p>The SAS Registry Database and SAS Node databases do not <i>store</i> or <i>retain</i> federal system information that is not specifically and positively permitted by Part 96 rule.</p> <p>Reference Section 6.4 (SAS User Access Services)</p> <p>SAS Nodes do not persistently <i>store</i> or <i>retain</i>, and do not <i>transmit</i>, information learned from a ESC.</p>

	Information learned by a SAS Node from a ESC and used in the calculation of spectrum availability may be <i>temporarily cached</i> (i.e. stored in volatile memory) in a SAS Node to improve the immediate performance of calculation. This transient information is available only to the caching software application and is destroyed after use.
--	---

§96.65 Spectrum access system administrator fees.

<i>(a) An SAS Administrator may charge Citizens Broadband Radio Service users a reasonable fee for provision of the services set forth in subpart F of this part.</i>	Reference Section 9 (Key Bridge SAS Commercialization Strategies) The 3.5 GHz ecosystem is emergent and rapidly evolving, as are various underlying commercialization strategies for fee recovery. Key Bridge may pursue several different commercialization strategies, each having its own fee collection process.
<i>(b) The Commission, upon request, will review the fees and can require changes to those fees if they are found to be unreasonable.</i>	Key Bridge understands and acknowledges the Commission's authority to review fees and to require changes to those fees if they are found to be unreasonable.

§96.66 Spectrum Access System Responsibilities Related to Priority Access Spectrum Manager Leases

<i>(a) An SAS Administrator that chooses to accept and support leasing notifications shall:</i>	Key Bridge SAS Infrastructure will accept and support leasing notifications.
<i>(1) Verify that the lessee is on the certification list, as established in section 1.9046 of this chapter.</i>	SAS Infrastructure will verify lessee certification either by confirming status as a Priority Access Licensee or as a ULS (form 608) certified entity.
<i>(2) Establish a process for acquiring and storing the lease notification information and synchronizing this information, including information about the expiration, extension, or termination of leasing arrangements, with the Commission databases at</i>	Key Bridge will establish a secure, daily process to acquire, store and synchronize lease notification information with the Commission. The developed lease notification synchronization process and data transfer scheme will be automated and machine-readable.

<i>least once a day;</i>	
<i>(3) Verify that the lease will not result in the lessee holding more than the 40 megahertz of Priority Access spectrum in a given License Area;</i>	<p>SAS Infrastructure will record the holdings of each lessee in the SAS Registry Database.</p> <p>Key Bridge will take care to ensure that no lessee holds more than 40 MHz of Priority Access spectrum in any given License Area (census tract).</p> <p>Key Bridge will also take care to ensure that violations of this requirement, be they inadvertent, purposeful, due to error or omission, will be rapidly and automatically corrected and reported to the Commission once discovered. Correction may be through the invalidation or reversal (i.e. unwinding) of a lease transaction agreement.</p>
<i>(4) Verify that the area to be leased is within the Priority Access Licensee's Service Area and outside of the Priority Access Licensee's PAL Protection Area; and</i>	<p>Reference Section 6.10.8 (PAL Protection Areas)</p> <p>SAS Infrastructure will verify that the geographic extent of all leases conforms with the Rules and are within the Priority Access Licensee's Service Area and outside of the Priority Access Licensee's PAL Protection Area.</p>
<i>(5) Provide confirmation to licensee and lessee whether the notification has been received and verified.</i>	<p>SAS Infrastructure will provide positive (or negative) notification to a Priority Access licensee and lessee when a leasing notification has been received and verified (or cannot be verified).</p> <p>Notifications will be made immediately upon acceptance, verification and processing by the SAS Infrastructure.</p>
<i>(b) During the period of the lease and within the geographic area of a lease, SASs shall treat any CBSD operated by the lessee the same as a similarly situated CBSDs operated by the lessor for frequency assignment and interference mitigation purposes.</i>	<p>A lease notification may stipulate a start-time and duration.</p> <p>SAS Infrastructure will extend Priority Access Licensee protections after a leasing notification is accepted (i.e. received, verified and processed) by the SAS Infrastructure for CBSDs operating within a leased geographic area and for the specified time period.</p> <p>If no time period is indicated then protections will be afforded immediately upon leasing notification acceptance and extended until either the original PAL expires or a subsequent notification of early termination is received by the SAS Infrastructure.</p>

2 Responses to Proposal Conformance Requirements

Below we respond, directly and briefly, to the specific requirements identified in the Commission's request for proposal. We also provide direct references to help the reader locate additional details in this proposal. Note that the direct references are indicative and not exclusive; they may be supplemented or supported by other aspects of the proposal and should be considered in the context of a end-to-end solution.

Wireless Telecommunications Bureau and Office of Engineering and Technology Establish Procedure and Deadline for Filing Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s) Applications

GN Docket No. 15-319 , DA 15-1426 , Released: 12/16/2015

ESC Operator Requirements And Functions

All proposals must at a minimum include the following information:

<i>1. A detailed description of the scope of the functions that the SAS and/or ESC would perform.</i>	Reference Section 5 (Key Bridge SAS High-Level Architecture) The proposed SAS will implement all aspects of allowed and envisioned Part 96 operation.
<i>2. A demonstration that the prospective SAS Administrator or ESC operator possesses sufficient technical expertise to operate an SAS and/or ESC, including the qualifications of key personnel who will be responsible for operating and maintaining the SAS and/or ESC.</i>	Reference Section 4 (Key Bridge Qualifications) Key Bridge is technically capable to develop, test and receive certification and to operate the described SAS Infrastructure solution indefinitely. Key Bridge is one of only five entities to have developed and received FCC certification to operate a TV-Bands spectrum administration system.
<i>3. The prospective SAS Administrator or ESC operator must demonstrate that it is financially capable of operating an SAS and/or ESC for a five year term.</i>	Reference Section 4.4 (Qualifications to Administer a SAS) Key Bridge is financially capable to develop, test and receive certification and to operate the describe SAS Infrastructure solution indefinitely. Key Bridge operates a profitable TV-Bands service.
<i>The proposal must include a description of the prospective SAS Administrator or ESC operator's business structure including ownership information.</i>	Reference Section 4.2 (Business Structure) and 4.3 (Key Personnel) Key Bridge Wireless LLC (fmr "Key Bridge Global LLC" and dba "Key Bridge") is a limited liability

	<p>corporation organized in the State of Virginia. Key Bridge is presently 100% owned by Mr. Jesse Caulfield, the sole managing partner.</p>
<p><i>To the extent that the proponent will rely on fees to support its operations, the proposal should also describe the fee collection process and the entities from which the fees will be collected.</i></p>	<p>Reference Section 9 (Key Bridge SAS Commercialization Strategies)</p> <p>The 3.5 GHz ecosystem is emergent and rapidly evolving, as are various underlying commercialization strategies for fee recovery. Key Bridge may pursue several different commercialization strategies, each having its own fee collection process.</p>
<p><i>4. A description of how data will be securely communicated between the SAS and its associated ESC and how quickly and reliably these communications will be accomplished.</i></p>	<p>Reference Section 7.2.4 (SAS to ESC Peering)</p> <p>SAS – ESC peering is a message-based open communications link. All transmissions are sender initiated (i.e. they follow a “PUSH” strategy) and messages are conveyed <i>immediately</i> to the receiver without delay.</p> <p>Reference Section 8.2 (Communications Security)</p> <p>Message reliability and information integrity is assured through the use of <i>WS-Security</i> authentication, integrity and confidentiality procedures.</p>
<p><i>5. Technical diagrams showing the architecture of the SAS and/or ESC and a detailed description of how each function operates and how each function interacts with the other functions.</i></p>	<p>Reference Section 5 (Key Bridge SAS High-Level Architecture) and 6 (Key Bridge SAS Concept of Operation)</p> <p><i>SAS Infrastructure</i> is implemented as a distributed application comprised of one or more <i>SAS Root Nodes</i> and a plurality of variously configured <i>SAS Nodes</i>.</p>
<p><i>6. A description of the propagation model and any other assumptions that the prospective SAS Administrator or ESC operator proposes to use to model operations and facilitate coordination in the band.</i></p>	<p>Reference Section 6.9.3 (Modeling Signal Propagation)</p> <p>Key Bridge proposes to use the IEEE 1900.5.2 strategy of a modeled path loss to provide mathematically robust, repeatable CBSD coexistence and frequency coordination calculations without external dependency on a digital terrain model.</p>
<p><i>7. A description of the methods that will be used to update software and</i></p>	<p>Reference Section 8.3 (Software Security)</p> <p>All software will be digitally signed. All applications</p>

<i>firmware and to expeditiously identify and address security vulnerabilities.</i>	will be configured with appropriate security permissions.
<i>8. An affirmation that the prospective SAS Administrator and/or ESC operator (and its respective SAS and/or ESC) will comply with all of the applicable rules as well as applicable enforcement mechanisms and procedures.</i>	<p>Reference Opening Letter.</p> <p>Key Bridge affirms that it is competent and will comply with all applicable rules and enforcement mechanisms and procedures in the operation of SAS Infrastructure.</p> <p>Key Bridge also affirms that it is competent and will comply with subsequent guidance, clarifications and decisions as may be issued from time-to-time by the Commission concerning operation of a SAS.</p>

SAS proposals must also provide the following information:

<i>1. A detailed description of how the SAS will retain, secure, and verify information from CBSDs (including location data), licensees, associated ESCs, and other SASs.</i>	<p>Reference Section 5 (Key Bridge SAS High-Level Architecture)</p> <p>The SAS Registry Database and SAS Node databases <i>store</i> licensee records and other information required by Part 96 rule.</p> <p>Reference Section 6.4 (SAS User Access Services)</p> <p>Only registered, authorized CBSDs may communicate and receive services from a SAS Node.</p> <p>Immediate CBSD operating information is <i>retained</i> within the CBSD's responsible SAS Node internal database.</p> <p>Reference Section 8.5 (Counter-Party Authentication)</p> <p>All communications with and within SAS Infrastructure are authenticated and <i>verified</i> using counter-party authentication with X.509 digital certificates.</p> <p>Reference Section 8 (Key Bridge SAS Security Architecture)</p> <p>All <i>communications</i> with and within CBRs systems are cryptographically protected. This includes all links and data exchanges to and between CBSDs, ESCs and SASs.</p>
---	---

<p><i>2. A demonstration that the SAS will be capable of resolving various sources of interference between and among Citizens Broadband Radio Service users and/or Incumbent users.</i></p>	<p>Reference Section 6.9 (Modeling and Computing Spectrum Coexistence)</p> <p>Key Bridge proposes to use the IEEE 1900.5.2 strategy to establish spectrum coexistence using modeled transmitters and receivers. The IEEE 1900.5.2 enables CBRS networks and populations of CBSDs to be readily modeled within a SAS Node and for coexistence calculations and analysis to be efficiently executed against the various CBSD models.</p>
<p><i>3. A description of how the SAS will ensure that non-federal FSS earth stations and grandfathered 3650-3700 MHz licensees are protected from harmful interference consistent with the rules.</i></p>	<p>Reference Section 6.7 (Protecting Non-Federal Incumbent Users)</p> <p>The details and methodology of how FSS protected contours are to be calculated is the subject of ongoing work by multi-stakeholder groups in which Key Bridge is a participant.</p>
<p><i>4. A description of how coordination will be effectuated (e.g., through data synchronization) between multiple SASs, if multiple SASs are authorized, and how quickly this synchronization of data will be accomplished.</i></p>	<p>Reference Section 7.3.2 (SAS to SAS Peering)</p> <p>SAS – SAS peering is a message-based communications link. All transmissions are sender initiated (i.e. they follow a “PUSH” strategy) and messages are conveyed <i>immediately</i> to the receiver without delay.</p>
<p><i>5. If the prospective SAS Administrator will not be performing all SAS functions, it must provide information on the entities operating other functions and the relationship between itself and these other entities.</i></p> <p><i>In particular, it must address how the Commission can ensure that all of the requirements for SAS Administrators in Part 96, subpart F are satisfied when SAS functions are divided among multiple entities, including a description of how data will be transferred among these various related entities and SASs, if multiple SASs are authorized, and the expected schedule of such data transfers (i.e.,</i></p>	<p>The proposed SAS will implement all aspects of allowed and envisioned Part 96 operation. The Key Bridge solution does not rely upon any other entity for SAS administration services.</p>

<p><i>real-time, once an hour, etc.).</i></p>	
<p>6. A description of the methods (e.g., interfaces, protocols) that will be used by:</p> <ul style="list-style-type: none"> (1) <i>CBSDs to communicate with the SAS;</i> (2) <i>the SAS to communicate with CBSDs;</i> (3) <i>the SAS to communicate with other SASs; and, if applicable,</i> (4) <i>the SAS to communicate with one or more ESCs.</i> <p><i>The prospective SAS Administrator must also describe the procedures, if any, which it plans to use to verify that a CBSD can properly communicate with the SAS.</i></p>	<p>Reference Section 7.3.1 (User Access Service)</p> <p>CBSD to SAS and SAS to CBSD communications is managed through <i>User Access Service</i> modules.</p> <p>Reference Section 7.3.2 (SAS to SAS Peering)</p> <p>Independent, autonomous SAS instances communicate and coordinate operations via <i>SAS to SAS Peering</i>.</p> <p>Reference Section 7.2.4 (SAS to ESC Peering)</p> <p>Independent, autonomous SAS and ESC instances communicate and coordinate operations via <i>SAS to ESC Peering</i>.</p> <p>Reference Section 8.5 (Counter-Party Authentication)</p> <p>SAS to CBSD communication is verified and authorized using counter-party authentication, which is established during CBSD registration and enrollment.</p> <p>CBSD registration and credentialing may be directly with a SAS or indirectly via a trusted third party network operator.</p>
<p>7. An affirmation that, consistent with section 96.55 of the Commission's rules, the SAS will only retain records and information or instructions received regarding federal transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process.</p>	<p>Key Bridge affirms that the SAS take care to handle information received from a ESC in accordance with information use policies conveyed by the ESC.</p> <p>Key Bridge expects that ESC policies will be established as part of the ESC approval process.</p> <p>Reference Section 5 (Key Bridge SAS High-Level Architecture)</p> <p>SAS Nodes are designed to reflect the immediate instructions and state information presented by a ESC. SAS Nodes are not configured with an ability to retain historical records of information received from the ESC.</p> <p>Centralized SAS systems such as the <i>Administration Portal</i>, the <i>Root Node</i>, a <i>Registry Database</i>, etc. will not have direct access to ESC transmissions. However these centralized systems and applications could potentially learn about ESC spectrum availability</p>

	<p>information updates during the course of normal operation; they are not configured to do so.</p> <p>Information retention policies implemented in these centralized systems will comply with whatever constraints are established and conveyed by the ESC. These retention policies and constraints are expected to be either a) fixed: established during the provisioning of a SAS to ESC peering session, or b) dynamic: embedded into the <i>SAS Gateway Protocol</i> used for information exchange between a SAS and ESC.</p>
<p>8. <i>A description of the security methods that the prospective SAS Administrator plans to use to ensure that unauthorized parties cannot access or alter the SAS or otherwise corrupt the operation of the SAS in performing its intended functions, consistent with the Commission's rules.</i></p>	<p>Reference Section 8.1 (Database Security)</p> <p>Key Bridge implements database security practices to ensure the integrity and confidentiality of system information.</p> <p>Reference Section 8.2 (Communications Security)</p> <p>All communications with and within CBRS systems are protected using cryptographic techniques such as counter-party authentication, transport and message layer security, etc.</p>
<p>9. <i>Descriptions of dynamic use-case scenarios for how the SAS will manage and assign spectrum resources to ensure that geographically and spectrally adjacent operations are coordinated consistent with the Commission's rules.</i></p> <p><i>Use case scenarios should include the methodology and protection approach for cases of radio interference due to adjacent blocking, out-of-band emissions, and aggregate co-channel interference.</i></p> <p><i>Describe how multiple SASs will coordinate the calculation of aggregate interference for protecting Incumbent users and Priority Access licensees.</i></p>	<p>Reference Section 6 (Key Bridge SAS Concept of Operation)</p> <p>A framework for SAS-to-CBSD communications is presently under study in a multi-stakeholder group chaired by Key Bridge. This work is in progress.</p> <p>Methodologies and protection strategies for handling adjacent blocking, out-of-band emissions and calculating aggregate co-channel interference are under study in a multi-stakeholder group in which Key Key Bridge is a member and participant. This work is in progress.</p> <p>Reference Section 6.4 (SAS User Access Services)</p> <p>In general CBSD to SAS spectrum services follows a client / server model, with the CBSD assigned the client role and typically initiating communication sessions with a SAS Node (server), which typically awaits incoming requests.</p>

	<p>Inter-SAS data exchange to facilitate the calculation of aggregate interference and the coordination necessary to protect incumbent and PA users is incorporated into the SAS Node request service process; inter-SAS coordination occurs in the SAS Node <i>Coexistence Engine</i> module.</p> <p>Reference Section Appendix: Femto Access Point Use Case</p> <p><i>User Access Service</i> configurations enable direct SAS interoperability with a variety of network access systems and technologies including <i>LTE eNodeB</i>, <i>WiMAX</i> base station plus <i>Femto Access Points</i> and <i>Home Node B</i> systems, among others using the existing operations and management protocols of those respective networking systems.</p>
<p>10. A description of the methods that the SAS will use to make information stored or retained by the SAS available in response to a request from authorized Commission personnel.</p>	<p>Reference Section 5.4 (SAS Portal)</p> <p>Key Bridge SAS Infrastructure will operate in a persistent, uninterrupted manner and will be available to provide any information it contains that the Commission may require.</p> <p>Key Bridge will provide access through one or more <i>SAS Portals</i> which Commission personnel may use without constraint. Personnel may also contact Key Bridge directly for any information or reports not otherwise available.</p>

3 Definitions and Abbreviations

This document incorporates by reference the various definitions relevant to operations in the 3.5 GHz band as provided by the FCC in 47 CFR 96.3. In addition, the following abbreviations are commonly used.

API	Application Programming Interface
CBRS	Citizens Broadband Radio Service
CBSD	Citizens Broadband Radio Service Device; a type of CRS
CRS	Cognitive Radio System
DFS	Dynamic Frequency Selection
DoD	U.S. Department of Defense
ESC	Environmental Sensing Capability
ETL	Extract-Transform-Load
EUD	End User Device
FAP	Femto Access Point, also called Femtocell
FCC	Federal Communications Commission
FSS	Fixed-Satellite Service
GA	General Authorized (typically when referring to a user)
GAA	General Authorized Access
IU	(Informing) Incumbent User; information is known <i>a priori</i>
LTE	Long-Term Evolution, marketed as 4G wireless service
NIIU	Non-Informing Incumbent User; information must be learned
NTIA	National Telecommunications and Information Administration
PA	Priority Access (typically when referring to a user)
PAL	Priority Access License
RLAN	Radio Local Area Network, also called Wireless Lan (WLAN)
SAS	Spectrum Access System
WBS	Wireless Broadband Service (FCC Rules Part 90, Subpart Z)

Table 1: Commonly used abbreviations

4 Key Bridge Qualifications

Established in 2001, Key Bridge Wireless LLC is a privately held Virginia small business providing spectrum administration, spectrum monitoring, professional services and online information services to the Telecommunications industry, the U.S. Government, and the U.S. Military.



Illustration 1: Summary of Key Bridge capabilities

Key Bridge offers a broad portfolio of turn-key information services, data processing and analysis engines, as highlighted in Illustration 1.

Since 2013 Key Bridge has provided flexible dynamic spectrum access services in the VHF + UHF television bands, ensuring the safety and uninterrupted delivery for billions of dollars in over-the-air entertainment, sports and news media services. Key Bridge is a leading TV band white space administrator and the Key Bridge White Space Database & Portal is the preferred solution for spectrum users to ensure uninterrupted wireless services. Our portals, spectrum data and database services support a diverse population of spectrum users in a trusted, neutral manner.

In addition to spectrum administration services Key Bridge also offers managed spectrum monitoring solutions based upon our custom designed embedded intelligent spectrum sensors. Key Bridge spectrum sensors may be deployed and connected over any standard TCP/IP network and provide high performance remote signal monitoring and real-time carrier detection.

4.1 The Key Bridge Team

Similar to our approach for the VHF + UHF frequency bands, Key Bridge has assembled a team of industry leading companies to provide a complete portfolio of technology, infrastructure, resources, expertise and personnel needed to develop, deploy and maintain a state-of-the-art SAS + ESC solution.

Key Bridge support operations will be contracted similar to our TV-Bands white space database support operations. The Key Bridge support team provides a robust and fully staffed operations center with established operating procedures, methods and practices that yield average service availabilities above 99.9%.



Illustration 2: Key Bridge SAS / ESC operations center.

Key Bridge continues to work with Oracle as our preferred supplier of commercial hardware and software technology. Oracle is one of the world's largest contributors of open source technology and also the owner and provider of the Java Developer Kit (JDK) and Runtime (JRE), Java Enterprise Edition (J2EE), Java Micro Edition (J2ME), and Java Card technologies.

For flexible compute, collocation and connectivity resources Key Bridge employs Amazon's cloud compute capabilities, which are supported by our own physical infrastructure co-located within Equinix facilities. Key Bridge has worked with Symantec since 2011 to incorporate

signed digital certificates, public key infrastructure and secure identity management in to our various spectrum administration solutions.

Oracle For almost 30 years, Oracle has helped customers manage their business systems and information with reliable, secure, and integrated technologies. Today, Oracle is the largest business software company in the world, with 345,000 customers - including 100 of the Fortune Global 100—and supports these customers in more than 145 countries.

Symantec Symantec (NASDAQ: SYMC) is one of the world's largest software companies with more than 17,500 employees in more than 40 countries. Symantec offers authentication solutions for government including PKI, two-factor authentication, and digital certificates that have been certified to meet the highest technical and policy standards of the United States Government.

4.2 Business Structure

Key Bridge LLC (fmr “Key Bridge Global LLC”, dba “Key Bridge”, “Key Bridge Wireless”) is a limited liability corporation organized in the State of Virginia. Key Bridge is 100% owned by Mr. Jesse Caulfield, the sole managing partner.

4.3 Key Personnel

Jesse Caulfield is the founder and CEO of Key Bridge Wireless LLC.

Mr. Caulfield has wide-ranging technical and business experience in cable, wireless and satellite service delivery. Mr. Caulfield chairs several industry groups, some specifically working to develop multi-stakeholder standards and standardized implementation guidelines for the emerging 3.5 GHz commercial ecosystem. Jesse frequently speaks at industry conferences and seminars and is widely recognized in the wireless community for his vision, thought leadership and expertise of dynamic spectrum access technologies and regulatory policy. Mr. Caulfield holds a degree in (High-Energy) Physics from the University of California, Los Angeles.

4.4 Qualifications to Administer a SAS

Key Bridge is technically competent and financially capable to develop, test and receive certification and to operate a SAS system indefinitely.

Key Bridge presently operates a profitable spectrum administration service for nearly 300 MHz in the VHF + UHF television broadcast bands and is financially capable of developing, testing and receiving certification and operating a SAS system to administer the 3.5 GHz band indefinitely.

In 2013 Key Bridge received FCC-certification to operate a TV-bands White Space database. While five other systems have since also tested and four received approval by the Commission, today Key Bridge is one of only three operators providing commercial white space administration services in the United States. A representative sample of companies and organizations that trust Key Bridge for spectrum administration services is shown in Illustration 3. *Note that no endorsement or relationship is implied or inferred.*



Illustration 3: Representative white space portal users.

Key Bridge white space administration is highly regarded in the industry. Presently over 150 companies and organization trust Key Bridge for neutral access to unlicensed spectrum and assured incumbent protection from interference, a degree of trust and reliance that exceeds all other administrators combined.

Key Bridge is able and intends to comply with all Commission rules, guidance and decisions related to a SAS, and asserts that Key Bridge is technically competent and financially able to operate a SAS in compliance with Commission rules.

5 Key Bridge SAS High-Level Architecture

In its 3.5 GHz Report and Order the Commission offered a normative concept architecture for a spectrum sharing configuration, shown in Illustration 4, that includes one or more Spectrum Access Systems (SAS) and a separate Environmental Sensing Capability (ESC).⁵ While not shown is it commonly understood that there may also exist multiple ESC implementations.

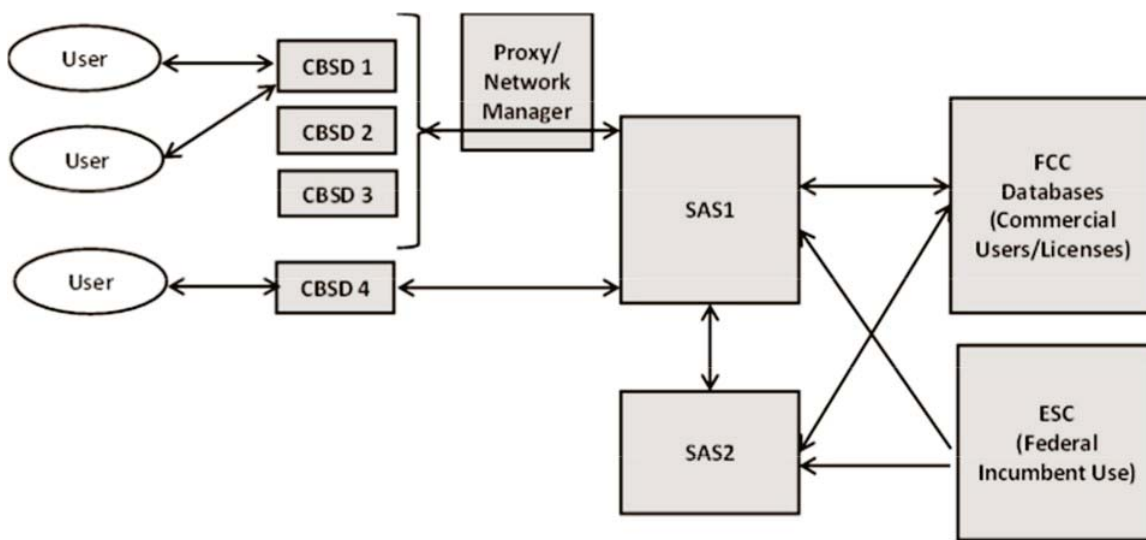


Illustration 4: Concept Citizens Broadband Radio Service architecture

To effectively coordinate Priority Access (PA) and General Authorized Access (GA) users in the 3.5 GHz band the SAS is responsible for authenticating and authorizing all CBSDs and ensuring that CBSDs operate within permissible technical parameters. In essence, the SAS's role is akin to frequency coordination but with a high degree of automation.

⁵ FCC Report and Order, Figure 3 at page 95.

5.1 SAS Information Architecture

Conceptually a SAS may be considered analogous to a “root” DNS, responding to spectrum resource queries according to various internal algorithms and calculations. These algorithms and calculations are influenced by external information learned from other SASs and from a ESC.

Different SAS and ESC implementations “peer” with each other and exchange messages via a SAS peering protocol. These peering messages facilitate data exchange and bilateral frequency coordination. The internal architecture and operations of the various SAS and ESC implementations are isolated from each other via the peering protocol.

SAS to SAS data sharing is still under development and remains the subject of debate. There are presently two schools of thought on SAS data sharing: a *unitary CBRS database* and a *partitioned CBRS database*. The Key Bridge SAS solution implements the “Partitioned CBRS Database” approach.

- **Unitary CBRS Database:** In a unitary database approach each autonomous SAS exports complete information to all peer SASs. In this model each SAS operates with exactly the same globally complete database. The TV-bands white space database is an example of a unitary database, where each administrator is obligated to offer exactly the same level of service to its users. The “Unitary CBRS Database” model freezes a single solution in place, discourages continuous innovation and is generally not compatible with competitive commercial service delivery; it is strongly disfavored.
- **Partitioned CBRS Database:** In a partitioned database approach each autonomous SAS encapsulates and does not export proprietary data (i.e. customer networks plus end user details). Each different SAS contains a “partition” of a global dataset and coordinates service delivery and user coexistence through a set of *peering* relationships. The “Partitioned CBRS Database” approach is loosely modeled on the global internet architecture where autonomous systems are responsible for their own internal operations (i.e. service delivery and management) and only expose summary information (i.e. aggregate routes) to other autonomous systems. This model promotes continuous technical innovation and commercial competition; it is strongly preferred.

The Key Bridge “Partitioned CBRS Database” SAS solution is designed as a distributed application comprised of intelligent, calculating, coordinating message processors. Each intelligent message processor is called a *SAS Node*. Key Bridge has incorporated lessons learned from the development, deployment and operation of our TV White Space system into an improved, second generation spectrum sharing solution that conforms with the Commission's conceptual SAS architecture (and coincidentally also the LSA concept architecture developed for the European market) and is or will be able to implement all of the Commission's prescribed and desired tasks and functions.

SAS Nodes are variably configured to provide a subset of the total catalog of available SAS functionality, services, tasks and responsibilities, according to their assigned role in the aggregate system. The sum collection of nodes are provisioned to establish a complete SAS functionality

and is called a *SAS Infrastructure*.

- **SAS Infrastructure** is a collection of SAS Nodes that, when operating together, provide a complete SAS functionality.
- **SAS Node** is a message and information processing application that provides one or more SAS services or functions.

5.2 SAS Infrastructure

Our “Partitioned CBRS Database” autonomous system is called a *SAS Infrastructure* and is summarized in Illustration 5.

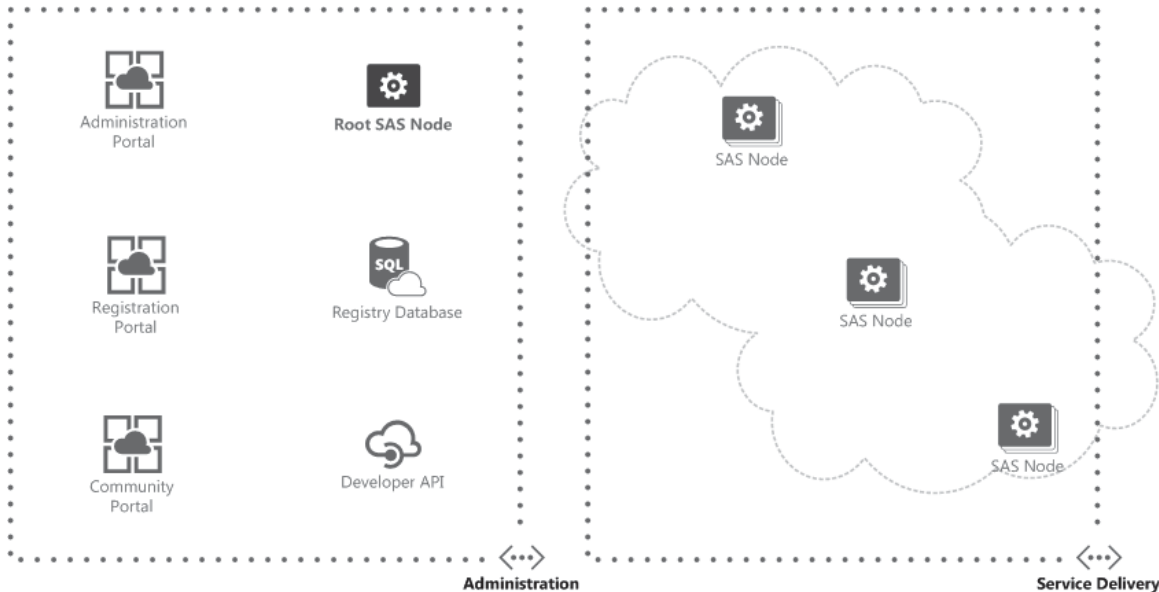


Illustration 5: SAS Administration and Service Delivery components.

Key Bridge SAS Infrastructure is realized as a distributed computer application comprised of one or more *SAS Root Nodes* and a plurality of variously configured *SAS Nodes*. SAS Infrastructure is functionally partitioned into Administration and Service Delivery components. Administration components include a *SAS Administration, Registration and Community Portal*, a *SAS Registry Database*, a *SAS Developer API* for automated machine-to-machine data exchange, and a *SAS Root Node*.

The SAS Infrastructure is managed through the *SAS Administration Portal*, and the *SAS Registry Database* contains a current snapshot of the global operating configuration plus all information identified in 96.55 except current information on registered CBSDs, which is stored in the local SAS Node database for each respective CBSD.

The various applications in the Administration and Service Delivery functional partitions are further logically partitioned into different enclaves called *security domains*. The current concept of operations (CONOPS) architecture and general partitioning strategy are further detailed in Section 8 (Key Bridge SAS Security Architecture), where the anticipated application relationships between the various SAS functional components is presented and their placement in different, layered security domains is indicated.

5.3 SAS Node

A *SAS Node* is a software application configured to process and/or route spectrum access messages and events. A SAS Node is designed around a *Coexistence Engine*, a *Data Processing* engine, and a *Data Storage* engine (i.e. a Database), with various other administrative and communications modules providing for remote access and service delivery capabilities. This concept is shown in Illustration 6 in a high-level, notional SAS Node architecture collaboratively developed and presented by Key Bridge in a multi-stakeholder group.⁶

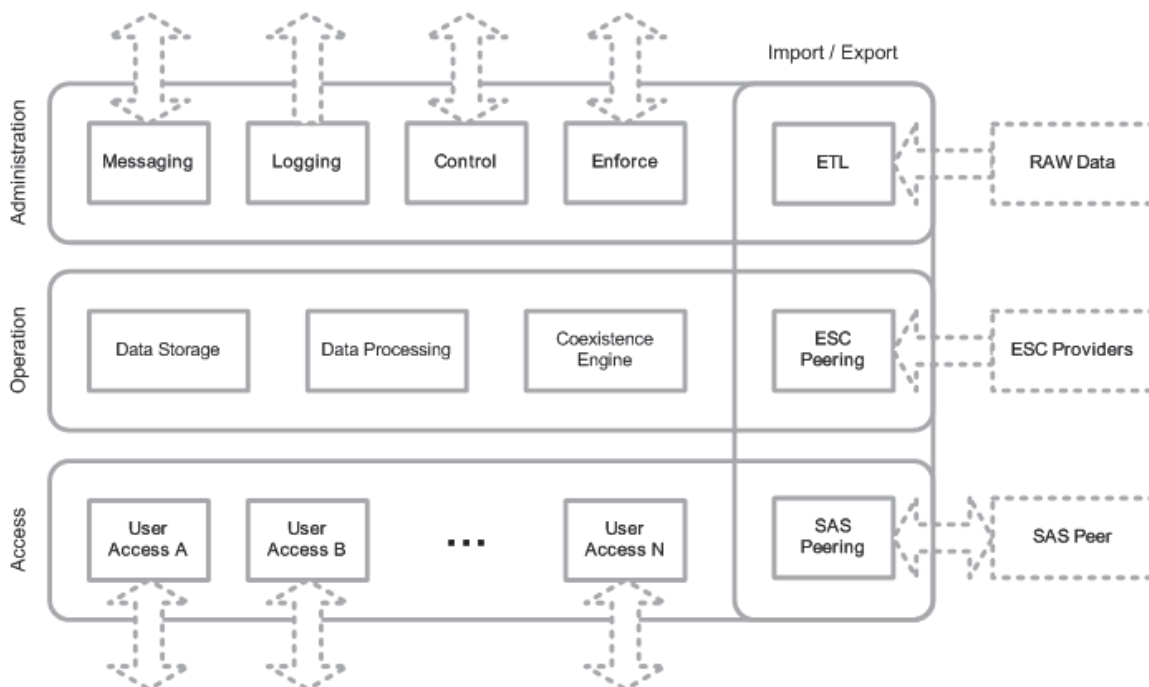


Illustration 6: A high-level, notional SAS Node architecture.

In the multi-stakeholder notional architecture and likewise in the Key Bridge SAS Node implementation there are several “Northbound” interfaces for SAS instance administration and management functions, “Eastbound” interfaces for operational data exchange with external systems, and “Southbound” interfaces for service delivery to different wireless networks and devices.

The Key Bridge SAS Node design builds upon this high-level, notional architecture with established industry standards, work-in-progress standards and best practice developments, plus lessons learned from our experience operating a TV-Bands database to implement a sophisticated frequency coordination and dynamic spectrum access capability.

⁶ The Wireless Innovation Forum, Spectrum Sharing Committee, Working Group 3: *Protocols and Data Formats*. (WG3)

5.4 SAS Portal

SAS Nodes individually plus SAS Infrastructure collectively will be generally managed and administered through a *SAS Administration Portal*. Non-federal incumbent and grandfathered wireless broadband service providers may register information in the SAS through a *SAS Registration Portal*. Non-administrative interaction with the SAS will be provided through a *SAS Community Portal*. These portals will be modeled on our existing white space portals, which provide feature-rich capabilities and are used by Key Bridge and our customers to interact with the Key Bridge White Space database system. A mock-up screen shot of a SAS Administration Portal is shown in Illustration 7.

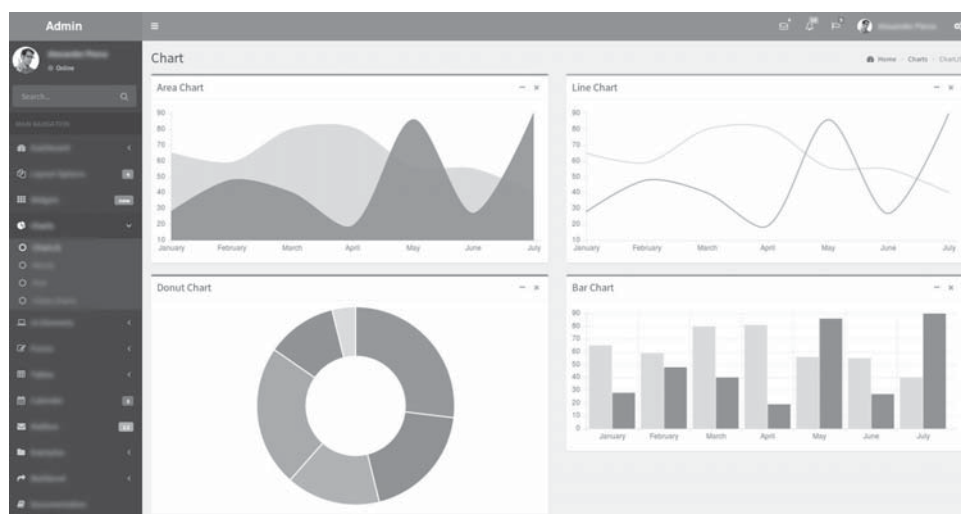


Illustration 7: Mock-up example of a SAS Administration Portal

Key Bridge expects to develop and operate several portal properties and online services in support of our SAS. These include:

- **SAS Administration Portal** provides global system administration, configuration management, performance monitoring and oversight.
- **SAS Registration Portal** provides information entry for informing incumbent users such as fixed satellite service stations and grandfathered wireless broadband licensees.
- **SAS Community Portal** provides public access and interaction with SAS Infrastructure for spectrum availability inquiries, status requests and other public information.
- **SAS Developer API** is an anticipated capability to facilitate automated public access and machine-to-machine interaction with the SAS Infrastructure. This is expected to provide the same or similar capabilities and information as are available through a SAS Community Portal, but in machine-readable formats.

Key Bridge web portals are built with industry standard Java EE technology and run on powerful

enterprise-grade application servers that allows for dynamic technology insertion and removal. Portal architecture enables new and custom features to be easily integrated to meet customer specific needs and requirements such as enhanced collaboration, configuration management and work flow automation.

Key Bridge portal products are generally provisioned and operated under the software as a service model and are accessed by users using a thin client via a web browser. An Internet portal is a software platform for building and presenting websites and on line applications, and software as a service, sometimes referred to as "on-demand software", is a applications delivery model in which software and associated data are centrally hosted on the cloud.

6 Key Bridge SAS Concept of Operation

Key Bridge expects the FCC to authorize more than one party to operate a SAS, and once operational these different SAS implementations will be both independent and autonomous. We furthermore expect that each of these different SAS implementations will have their own internal databases of PA users, GA users and other operational state information, and may coordinate and cooperate with each other through inter-administrator peering.

This partitioned CBRs database concept, where different internal data sources may be coordinated across multiple independent SAS instances, is enabled by a robust peering strategy. This concept is shown in Illustration 8 and is an essential capability for seamless interoperability of CBSDs in the 3.5 GHz band.

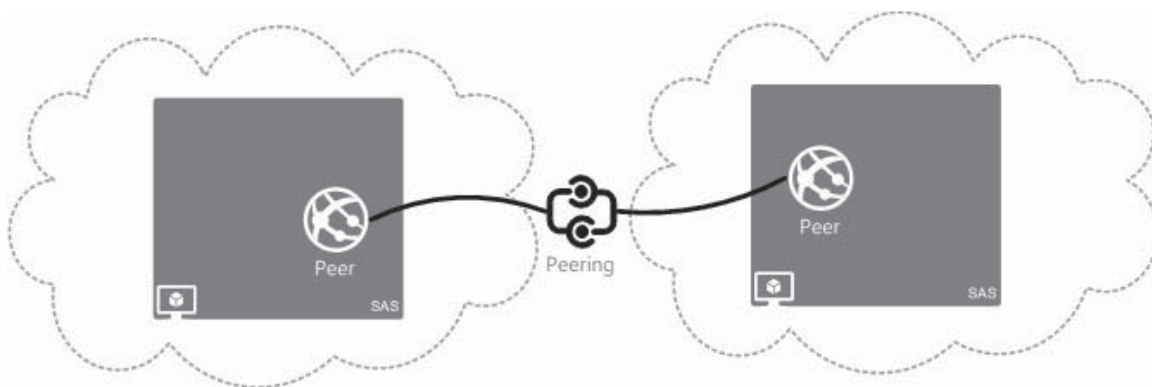


Illustration 8: SAS to SAS peering enables cooperation and collaboration.

Internally, a Key Bridge *SAS Infrastructure* is implemented as a distributed application comprised of one or more *SAS Root Nodes* and a plurality of variously configured *SAS Nodes*. In the Key Bridge SAS Infrastructure each SAS Node is configured to provide a subset of SAS services according to its prescribed role in the aggregate system. A Key Bridge *SAS Node* is a software application configured to process and/or route spectrum access messages and events and comprises a *Coexistence Engine*, a *Data Processing engine*, an internal *Database* and various “Northbound” administrative, “Eastbound” data, and “Southbound” user access services.

6.1 A Distributed, Meshed, Peer to Peer Application

Each *SAS Node* in a Key Bridge *SAS Infrastructure* is configured to provide a subset of (i.e. one or more) SAS functions and services from the complete set of SAS tasks and capabilities. In this way the Key Bridge SAS Infrastructure may also be thought of as a collaborative peer-to-peer computing application where tasks and work loads are distributed and assigned amongst different network hosts. In this way SAS Nodes are both suppliers and consumers of resources to the SAS Infrastructure. This model contrasts with a traditional client-server model in which computing resources are vertically divided, or with a traditional load-balancing model in which resources are horizontally spread across multiple systems.

Example application architectures using these different concepts are shown in Illustration 9 to provide more context.

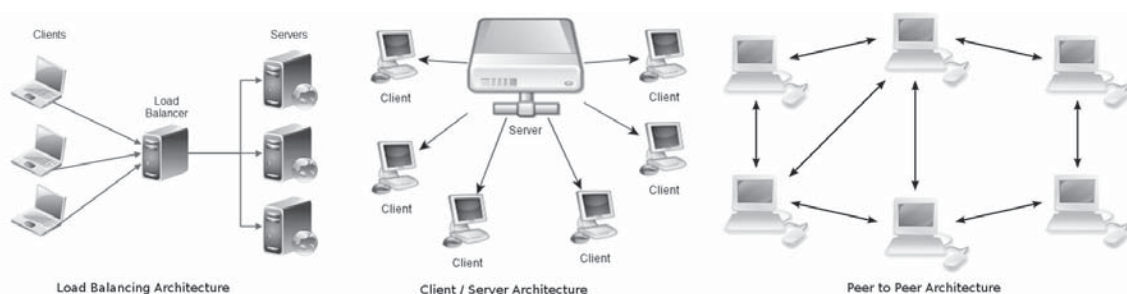


Illustration 9: Common application deployment scenarios.

A SAS Node in the SAS Infrastructure may be configured to service a limited geographic region, and set of channels, a PAL licensee, a particular GA device type, etc.

SAS Nodes communicate with other nodes via routed messages and cooperate to provide SAS Infrastructure services. Any request for service received by one SAS Node that lies outside that node's configuration is routed to another SAS Node having an applicable configuration compatible with the request. If no SAS Node is compatible with the request or is otherwise available the request is routed to a Root SAS Node, which is able to handle all requests.

6.2 Implementation Example

This concept may be further explained through example by referring to Illustration 10 where a SAS Infrastructure is shown comprised of numerous SAS Nodes in a geographic load balancing configuration. In the provided example each SAS Node is configured to provide services for a single user type in a progressively more specific geographic area of responsibility.

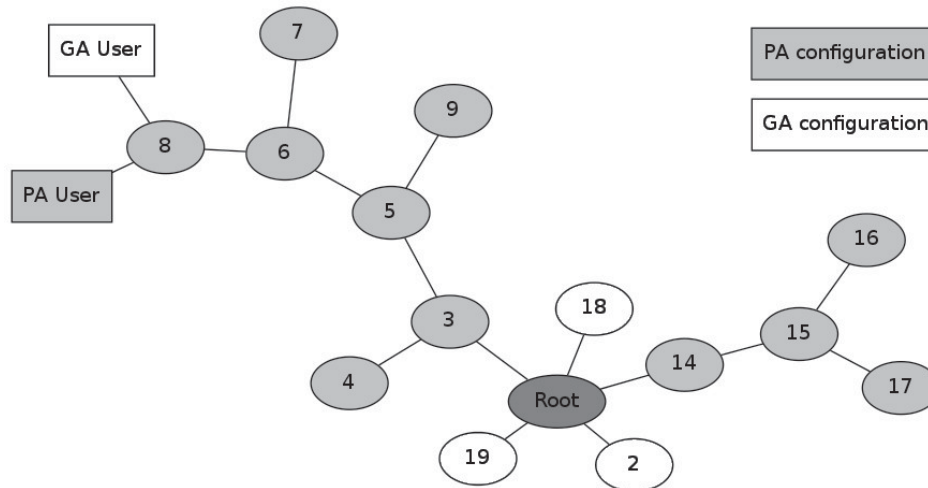


Illustration 10: SAS Infrastructure is a network of SAS Nodes.

Referring to the illustrated example: SAS Node #8 (in the upper left corner) may be configured to serve only PA users within a single facility, such as a conference center; SAS Node #6 may service PA users throughout the census tract containing the conference center; SAS Node #5 may serve PA users in the local county containing the census tract, and SAS Node #3 may serve PA users in the state, and finally the Root SAS Node serves all users of all types, globally. The Root SAS Node in this example has also spawned nodes #2, #18 and #19 to service GA users, globally.

It will be instructive to examine the scenario where a PA and GA user user requests service to SAS Node #8.

Referring again to Illustration 10, the PA user request to SAS Node #8 may be immediately processed by SAS Node #8, whereas a GA user request for service is outside the configuration of SAS Node 8 and routed “upstream” for processing. Continuing the example: the GA request for service to SAS Node #8 is routed to SAS Node #6, which is also not configured for GA service, then to SAS Node #5, then to SAS Node #3, then to the SAS Root Node, and finally to one of SAS Nodes #2, #18 or #19 for processing. The GA service message response path is the request path in reverse; SAS Node #8 remains the responsible handling end point for the GA service transaction.

By this method the internal operations of the SAS Infrastructure, specifically its internal message

passing and geographic load balancing strategy, are hidden from the PA and GA user, which both receive full, non-discriminatory 3.5 GHz services from the Key Bridge SAS Infrastructure.

To explain this concept further an example is shown in Illustration 11 for a hypothetical Key Bridge SAS Infrastructure servicing the state of Virginia, where a *SAS Root node* is configured to have global authority for all GA and PA users in the State of Virginia and is capable of servicing all user requests. A plurality of other SAS Nodes is then be provisioned to support, for example, increased general demand, regionally specific characteristics such as increased population density, the particular needs of a PA licensed operator, etc.

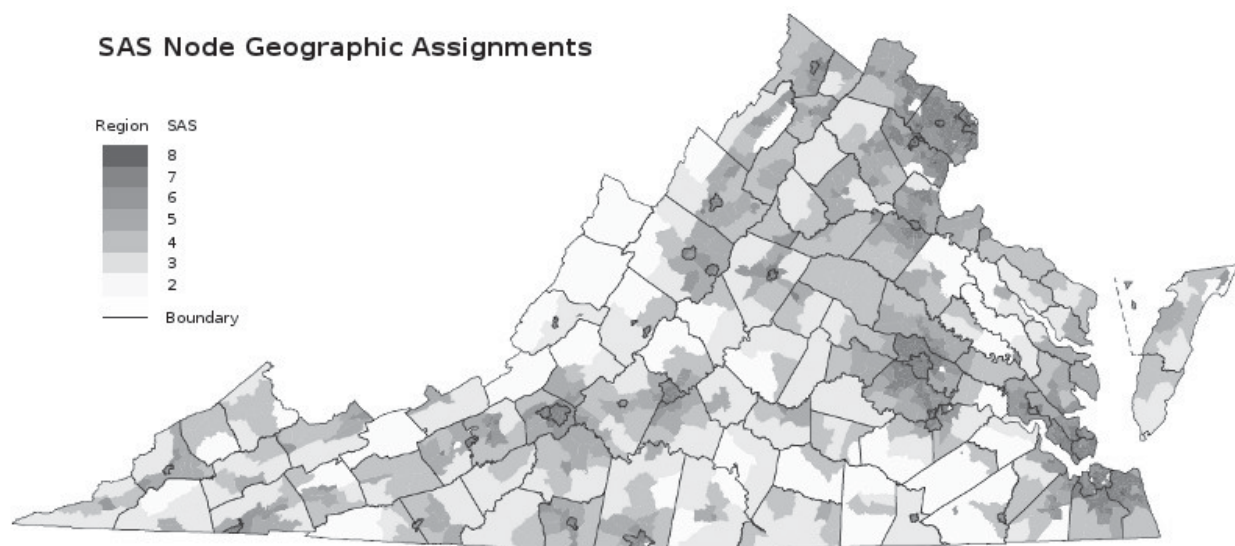


Illustration 11: SAS Nodes are dynamically provisioned for real-world demand.

In the illustrated example eight SAS Nodes are configured to provide service across the state of Virginia: seven nodes (numbered 2 through 8) that provide geographic partitioning (i.e. load balancing) and regionally specific or licensee-specific SAS features and services, plus a Root SAS Node that is not shown but always implied.

In this section we describe how a SAS Node singularly or, in collaboration with other SAS Nodes collectively, implements various SAS tasks and responsibilities.

6.3 Message Oriented Communications

In a SAS Node the sending software module (i.e. a User Access Service, a SAS Peering module, etc.) initiates and controls the conveyance of information with other parties using a message exchange pattern called *message oriented communications*.

In a message oriented communications environment it is often necessary to assure that messages are actually received and processed successfully to ensure complete message passing and processing. SAS Node communications generally adhere to several important design patterns governing how information is exchanged including *transaction-based*, *at-least-once* and *exactly-once* message delivery.

6.3.1 Transaction-based Delivery

Message transactions should generally provide some assurance to the sending party that the message content was received intact and handled according to a prescribed process by the receiving party. All SAS Node and CBSD messages are therefore exchanged under a transactional context to ensure that messages are completely received and correctly processed.

When using transaction-based delivery the sender and the receiver participate in a transaction and all operations involved in the message exchange are performed under one transactional context. This concept provides *ACID* behavior and is shown in Illustration 12.

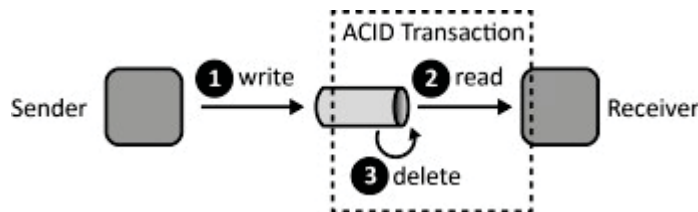


Illustration 12: Transaction-based message delivery pattern.

ACID (*Atomicity, Consistency, Isolation, Durability*) is a set of properties typically used in database systems to describe an information transaction having guaranteed, reliable and correct processing. For example, in the context of a database a single logical operation such as a READ or WRITE instruction is called a “transaction”. In a SAS, the transaction is a message exchange and includes information transfer, information parsing plus information handling and processing.

6.3.2 At-least-once Message Delivery

SAS Nodes attempt to ensure that a messages are delivered at least once to their intended recipient. This is implemented by automatic acknowledgement to the sender of each message retrieved by a receiver. If an acknowledgement is not received within a certain time period the message is automatically resent. That is: SAS node messages are automatically retransmitted to assure they are delivered at least once in case of failures that may lead to message loss or

timeout.

Message recipients automatically acknowledge message receptions to ensure that messages are received properly. To assure that a message is properly received it is not deleted by the sender immediately after it has been read by a client, but is instead marked as being *invisible* and held for completion. If the client fails to acknowledge the message it is marked *visible* and re-initiated. This process is outlined in Illustration 13.

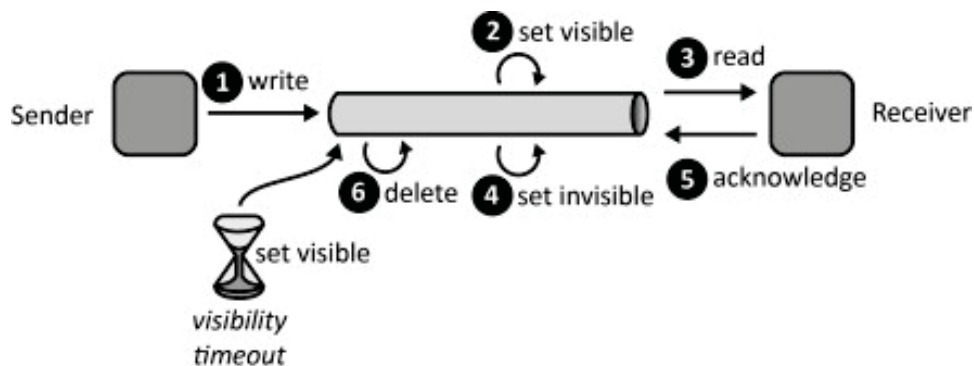


Illustration 13: At-least-once, exactly-once message delivery pattern.

After a client has successfully processed a message it sends an acknowledgement to the sending party, whereupon the message is deleted and the transaction may be closed.

6.3.3 Exactly-once Delivery

It may occur that messages are duplicated and more than one message may arrive to a recipient. For CBSD systems any duplicate SAS response message is not acceptable, and for SAS Nodes duplicate input messages may be confusing and difficult to process.

SAS Node messaging handles message duplication through the use of message identifiers, where each message is associated upon creation with a globally unique message identifier. This identifier is used to filter message duplicates during their traversal from sender to receiver. This message design pattern is called *exactly-once* delivery.

6.4 SAS User Access Services

A general framework for SAS-to-CBSD communications is presently under study in a multi-stakeholder group chaired by Key Bridge. This work is in progress and not yet complete. Here we describe, in broad terms, how a normative CBSD is expected to interact with and receive service from a SAS Node.

In general CBSD to SAS spectrum services follows a client / server model, with the CBSD assigned the client role and typically initiating communication sessions with SAS servers, which typically awaits incoming requests and either directly responds or, if unable or otherwise configured, coordinates a response to those requests.

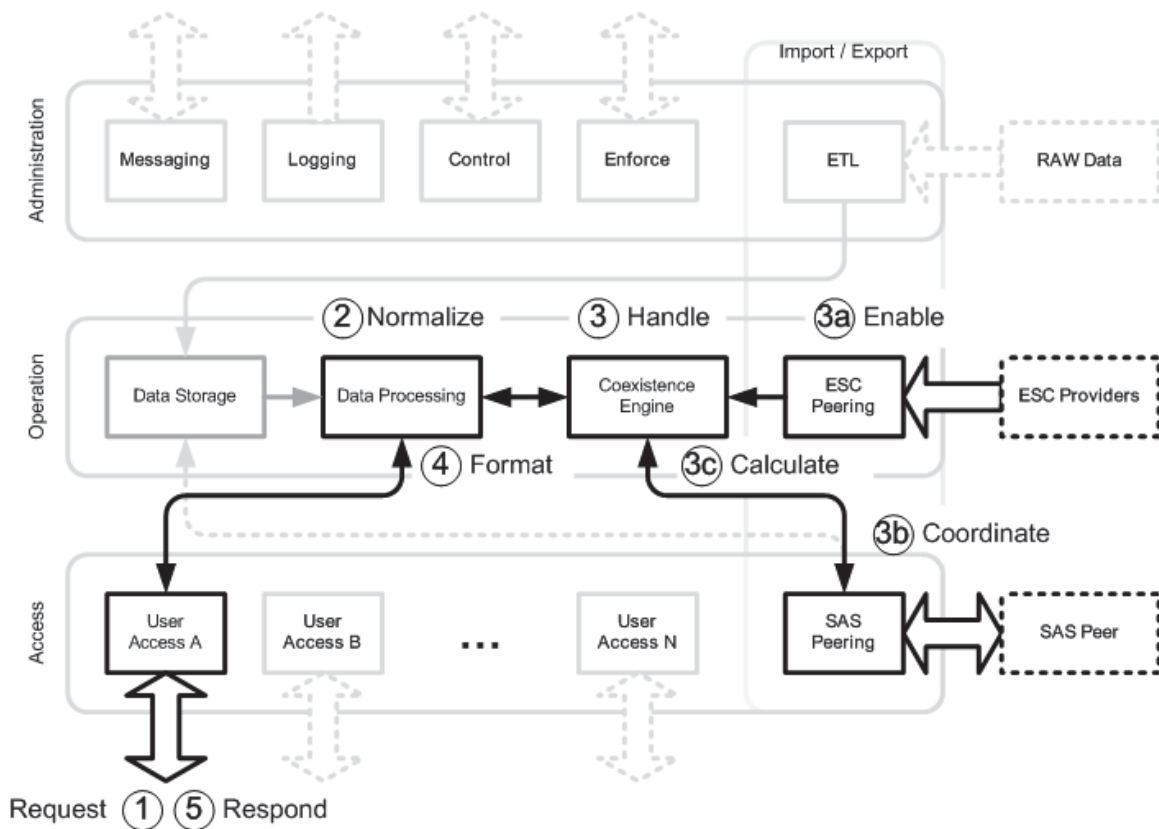


Illustration 14: SAS Node spectrum service handling.

User Access Service configurations are anticipated to eventually enable SAS interoperability with a variety of network access systems and technologies including *LTE eNodeB*, *WiMAX* base station plus *Femto Access Points* and *Home Node B* systems, among others. User Access Services for these specific network types are discussed further in 7.3.1 (User Access Service). In Illustration 14 we describe, in general, how a generic CBSD may receive spectrum information from a SAS Node by submitting a service request message to, and receiving a service response message from, a modeled SAS Node.

A summary of the SAS Node service delivery process is shown in Illustration 14 and proceeds according to the following steps:

1. **Request.** One of potentially several *User Access Service* modules receives a request for SAS services from a certified, authorized CBSD. The request is authenticated, authorized and validated by the *User Access Service* module and then forwarded to a *Data Processing* module for handling.
2. **Normalize.** The *Data Processing* module transforms the incoming service request into a normalized, standardized internal representation. The request is further validated and possibly supplemented with information from *Data Storage*, then forwarded to a *Coexistence Engine* for handling.
3. **Handle.** The *Coexistence Engine* module handles the service request, which includes applying local access and availability policies, retrieving information from ESC and other SAS entities, and conducting spectrum coexistence calculations.
 - a. **Enable.** If a ESC provider is available then the *Coexistence Engine* may query and retrieve ESC spectrum availability (enable) information from a *ESC Peering* module and apply that information as a filter to the immediate service request.
 - b. **Coordinate.** If the service request requires additional information or may affect the operations of other CBRS users the *Coexistence Engine* may initiate an external coordination transaction with other SAS Nodes or SAS instances through a *SAS Peering* module.
 - c. **Calculate.** Based upon all available information a immediate spectrum availability configuration is calculated by the *Coexistence Engine* module. This calculated result is then returned to the *Data Processing* module using a normalized, standardized internal message response format.
4. **Format.** The *Coexistence Engine* response information received by *Data Processing* module is again validated and possibly supplemented with user-specific information and other needed data from *Data Storage*, then formatted into a query response and forwarded to the User Access module.
5. **Respond.** Finally, the originating *User Access Service* module receives and correlates a complete spectrum query response message from *Data Processing* module and formats this information into a client-specific service response.

Recalling that User Access Service modules are configured to interface with different network architectures, by this method a Key Bridge SAS node may be configured to provide frequency coordination and to facilitate coexistence between any number of different, otherwise incompatible network architectures, operators and technologies.

6.5 Facilitating CBSD Coexistence

In this section we discuss several methods the SAS Infrastructure may use to facilitate CBSD coexistence. Implementation of the described coexistence strategies is ongoing and may necessarily include proprietary or protected methods and strategies.

Citizens Broadband Radio Service Devices (CBSDs) are by definition also a Cognitive Radio System (CRS) and must coexist (i.e. share spectrum with or operate in close spectral proximity to) other radio systems that are not necessarily cognitive, such as a incumbent transmitter and also with other radio systems that may have a greater priority access right to the spectrum, as well as with other co-equal devices. This complex, multi-tiered spectrum coexistence scenario can be modeled as a combination of two types of coexistence strategy: *horizontal* and *vertical*, which are shown in Illustration 15.

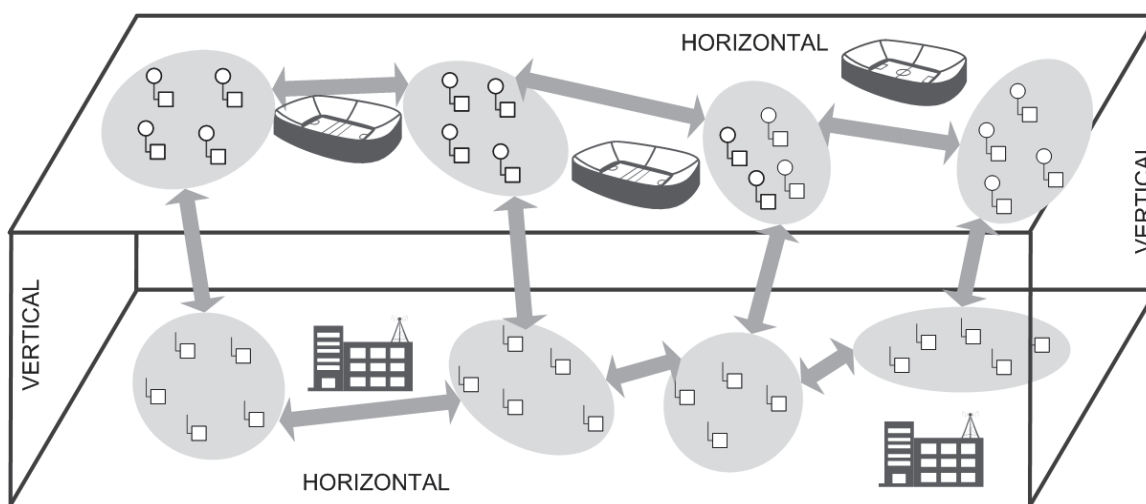


Illustration 15: Horizontal and vertical spectrum sharing strategies.

Vertical and horizontal spectrum sharing strategies are not mutually exclusive and may be implemented singularly or combined to establish a coexistence policy that is appropriate to whatever scenario a particular spectrum band may exhibit.

- **Horizontal spectrum sharing** is a scenario where multiple cognitive radio systems access the same shared spectrum band. In horizontal spectrum sharing all users have equal spectrum access rights but may have completely different access needs.
- **Vertical spectrum sharing** occurs when cognitive radio systems attempt to share a spectrum band with another radio system that may not have spectrum sharing capabilities or may enjoy superior access privileges to the spectrum. In a vertical sharing scenario devices with inferior access rights may access and use spectrum resources subject to certain constraints, such as obeying geographic exclusion zones, avoiding harmful interference, etc.

In the U.S. 3.5 GHz band PA – PA and GA – GA user coexistence would be forms of horizontal sharing, whereas PA – GA coexistence would be a form of vertical sharing.

While horizontal and vertical radio implementations in the 3.5 GHz band are still under development, Key Bridge SAS technology is designed to support and facilitate efficient spectrum use for whatever heterogeneous radio environment emerges in the 3.5 GHz band.

Below we describe several methods under consideration for how SAS Nodes may facilitate automated heterogeneous coexistence and coordination through combinations of horizontal and vertical spectrum sharing. It should be noted that the described methods are equally applicable to horizontal sharing (i.e. GA-GA and PA-PA coexistence) as they are with vertical sharing (GA-PA and CBSD-Incumbent).

6.5.1 Control Channel Messaging

SAS Nodes enable CBSDs to learn about their operational and geographical environment, identify and apply policies and establish an internal operating state. SAS Nodes support this capability through the exchange of secure information messages between heterogeneous networks and network management systems. In this context SAS Nodes act as a neutral broker between otherwise incompatible or potentially competing networks and radio systems, and enable the exchange of *control channel* messages and *pilot channel* messages.

Control channel messages are exchanged between radio devices or radio management systems, and the duplex exchange path is called a *control channel*. A primary use of control channels is to enhancing coexistence between secondary systems using the same spectrum resources, i.e. horizontal sharing between two networks with equal access privileges operating in the same geographic region and frequency band. An example configuration of this concept is shown in Illustration 16.

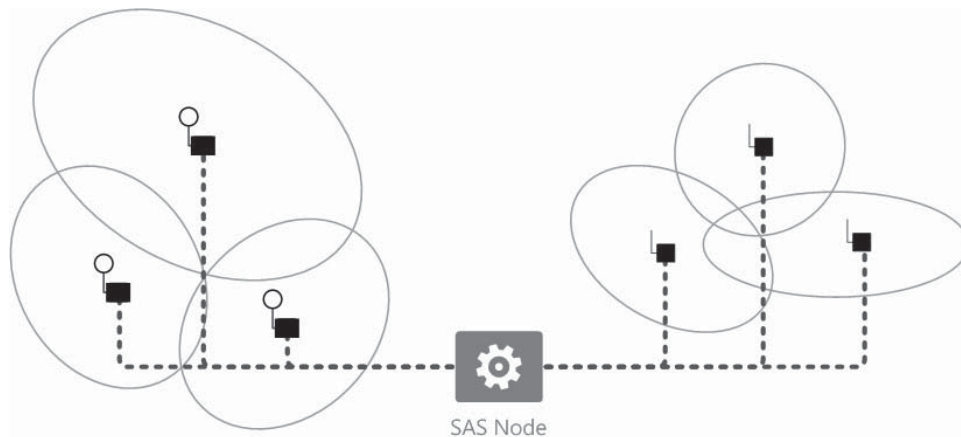


Illustration 16: Cognitive control channel to enhance heterogeneous network coexistence.

Control channel messaging involves the exchange of network operating control (i.e. management) information between otherwise isolated, autonomous (i.e. competing) and possibly heterogeneous (i.e. incompatible) systems that seek to use the same spectrum resources. SAS Node Control channels facilitate more efficient radio operation, spectrum use and coexistence of otherwise otherwise incompatible cognitive radio systems. SAS Nodes enable those systems to exchange information about local spectrum data and to directly negotiate operational configurations through the use of neutral coordinating signals that would otherwise be impossible.

SAS Node control channel messaging enables different CBRS Networks and devices to exchange real-time operating information such as current spectrum use, desired and required spectrum resources, sharing policies, and coexistence capabilities. SAS Node control channel messaging can support or facilitate many different coexistence functions, including:

- **Sharing and Coexistence:** providing information about local network capabilities, device spectrum needs and current use, and negotiating spectrum use with neighboring CRS devices;
- **Cooperative Sensing:** Synchronizing quiet periods to listen for radio signals that are not participating in a control channel coexistence scheme, for supplementing the spectrum sensing capabilities of neighbor devices to identify hidden nodes, and to coordinate with other neighboring network;
- **Network Clustering:** Off-air discovery of available networks or devices within range to connect to, and negotiating a radio link configuration with those networks or devices prior to transmission;
- **Spectrum Policy:** Receiving spectrum use and sharing policies rules for their immediate and local operating area. This may include certain bands or power limitations, special event exclusions, etc.

SAS Nodes provide control channel messaging as a neutral, trusted intermediary between anonymous end devices and network operators. Various 3.5 GHz devices, including CBSDs, CBSD networks, and legacy wireless devices and networks may exchange control channel information using the local SAS Node as an intermediary broker.

Control channel messages may be exchanged bilaterally between two administrative systems in a configuration as shown in Illustration 16 or may alternatively be distributed throughout a geographic area as shown in Illustration 17. SAS Infrastructure supports both a *direct* and a *distributed* mode of operation.

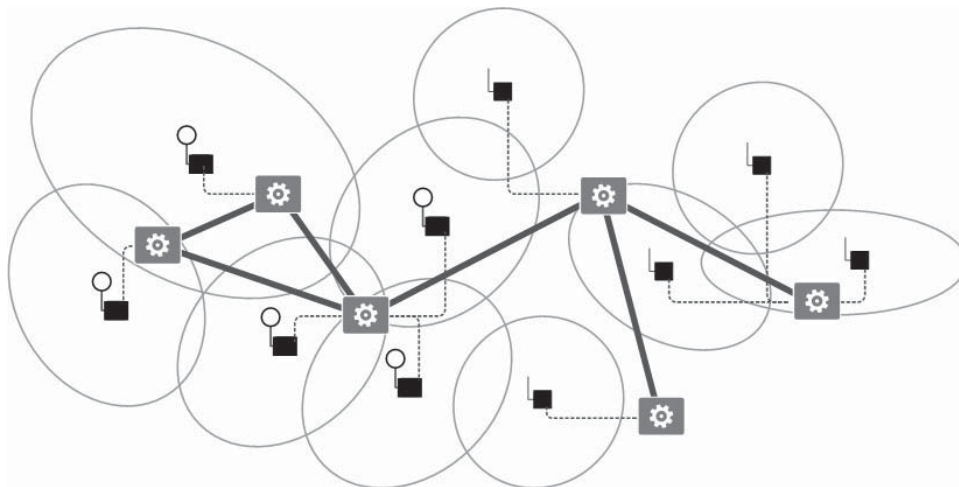


Illustration 17: Control channel information may be distributed via a mesh overlay.

Control channel information is protected using *message layer security*.

In this context the SAS Infrastructure acts as a *Message Oriented Middleware (MOM)*. MOM-

based systems allows communication through the asynchronous exchange of messages. Message Oriented Middleware makes use of messaging provider to mediate messaging operations. The basic elements of a MOM system are clients, messages, and the *messaging provider*, which includes an API and administrative tools. This concept is shown in Illustration 18.

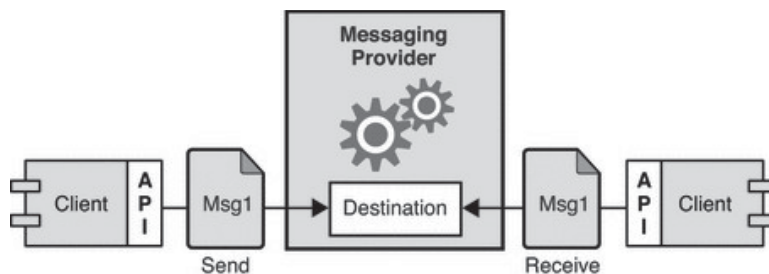


Illustration 18: Message exchange system.

Using a MOM system, a client makes an API call to send a message to a destination managed by the provider. The call invokes provider services to route and deliver the message. Once it has sent the message, the client can continue to do other work, confident that the provider retains the message until a receiving client retrieves it. The message-based model, coupled with the mediation of the provider, makes it possible to create a system of loosely-coupled components. Such a system can continue to function reliably, without downtime, even when individual components or connections fail. A compelling advantage of mediated messaging between clients is client applications are effectively relieved of every problem except that of sending, receiving, and processing messages.

Spectrum sharing participants in a control channel message exchange, such as a CBSD devices and networks, are called *control channel participants* (CCP). Control channel operation can be organized in three phases: *initialization*, *discovery*, *exchange*.

- **Initialization:** During control channel initiation the CCP registers with a SAS Node via an out of band path such as the Internet. CCP registration includes geo-location and other spectrum-related parameters. CCP entities may also include in their registration information about how to connect to the CCP entity, e.g. its network address, operating frequency, and necessary credential information.
- **Discovery:** Once registered a CCP discovers other CCPs in its geographic area by receiving update messages from the SAS Node. The CCP entity is regularly updated by the SAS Node and the CCP may discover new CCPs as they become available or may update existing CCPs as they become unavailable. Discovery messages may also include information about how to connect to the identified CCP.
- **Exchange:** Once discovered a CCP may exchange whatever control information may be required or desired through the SAS Node. The SAS Node acts as a trusted, neutral intermediary, isolating the two communicating end points from each other and providing a degree of anonymity and autonomy.

6.5.2 Pilot Channel Messaging

Pilot channel messaging involves the broadcast of information about the local radio operational environment to all interested parties within a geographic region. The one-way message exchange between the sender and receiver is called a *pilot channel*. Pilot channel messaging may be delivered directly (i.e. unicast) or indirectly broadcast (i.e. multicast). The geographic extent of a pilot channel may be dynamically adjusted according to the needs of the system. An example configuration is shown in Illustration 19, where a *pilot channel messenger* is employed to assist the responsible SAS Node with message distribution and delivery. In the example illustration the pilot channel messenger is a simple message repeating application that redirects unicast SAS Node messages to a local IP multicast stream.

SAS Nodes support pilot channel messaging as a neutral, trusted data publisher.

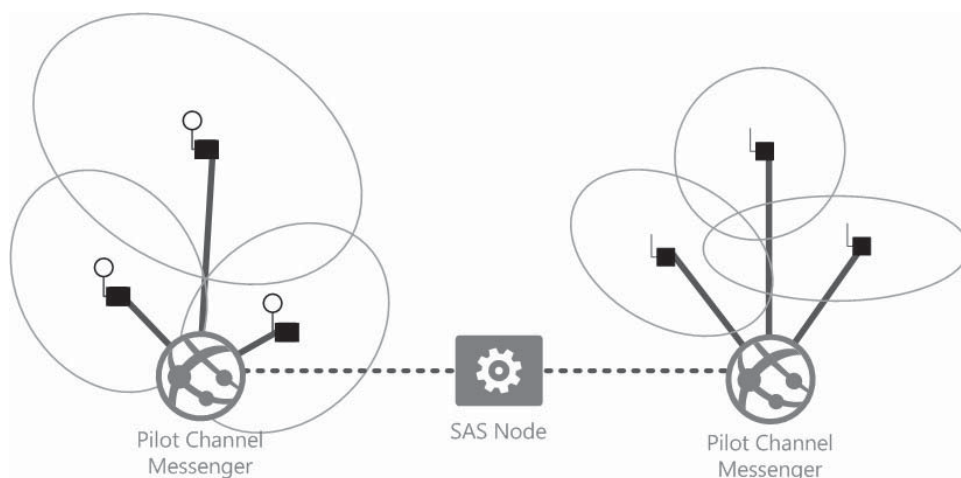


Illustration 19: Pilot channel messaging.

Pilot channel messages are useful for a CBSD to establish an initial configuration when operating in a complex or constrained radio environment. Pilot channel messages may include information such as the identity and network address of locally responsible SAS Nodes, regional spectrum use policies, channel allocation and assignment plans, plus presently assigned frequencies in a geographic region. These factors may all assist and promote efficient CBSD spectrum discovery and use.

In the 3.5 GHz band a pilot channel aids cognitive radio decisions in a dynamic and flexible heterogeneous spectrum environment that may also include non-informing or non-cooperative radio services within a defined geographic area. In some radio environments a CBSD may require current and regularly updated spectrum and radio environment information within an extended geographic region and operating frequency range. This may be supported by subscribing to one or more pilot channels of Key Bridge SAS Nodes or to a single SAS Node with sufficiently broad responsibility to achieve the logical coverage desired.

SAS Node pilot channel messaging is a out-of-band publish/subscribe messaging scheme with information limited to a certain geographical area (i.e. using a cellular approach). In this context out-of-band means that messages are delivered via a wired, not wireless communications path.

Pilot channel information is protected using *message layer security*.

Similar to its role as a Control Channel Broker, in this context SAS Infrastructure acts as a *message broker* providing a distribution mechanism for publishing messages that are delivered to multiple subscribers. This concept is shown in Illustration 20.

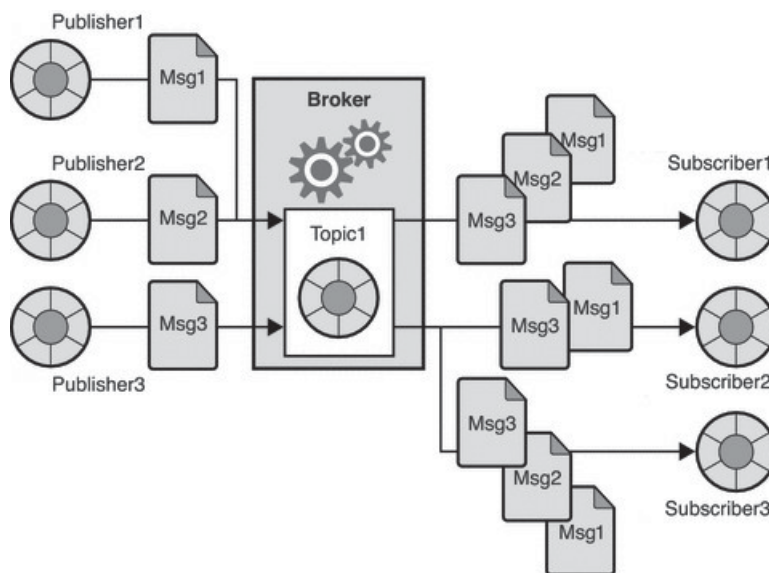


Illustration 20: Message publish/subscribe system.

In the publish/subscribe domain message producers are called *publishers* and message consumers are called *subscribers*. While the publish/subscribe model does not require that there be more than one subscriber, three subscribers are shown in the figure to emphasize the fact that this domain allows you to broadcast messages. All subscribers to a pilot channel (Topic1 in the illustration) get a copy of any message published to that pilot channel.

A main advantage of using a message broker and publish/subscribe model is that it allows messages to be broadcast to multiple subscribers. Other advantages include:

- More than one SAS Node can publish messages.
- More than one CBSD can consume messages. Subscribers may apply variable filters to limit the messages they receive.
- The broker can retain messages for subscribers while these subscribers are inactive.
- Publishers and subscribers can be added and deleted dynamically, thus allowing the messaging system to expand or contract as needed.

Spectrum sharing participants in a pilot channel message exchange, such as a CBSD devices and

networks, are called *pilot channel subscribers*. SAS Node pilot channel use can be organized in two phases: *initialization* and *update*.

- **Initialization:** When a CBSD device or network (e.g. terminal) wishes to receive pilot channel information it registers as a subscriber with a SAS Node. Registration includes the CBSD position or geographical area of operation. Following successful registration the SAS Node will send to the subscribing entity a comprehensive report containing spectrum-related and sharing information corresponding to the area where the subscriber is located, including present channel occupancy, policies in force, plus other useful empirical metrics and configuration information.
- **Update:** Once registered the subscriber will receive period messages from the SAS Node containing incremental updates to previously conveyed information. By this method a pilot channel subscriber may establish and maintain visibility to spectrum operations external to itself.

6.6 Protecting Federal Incumbent Users

ITU allocations for the 3.5 GHz band vary internationally. They are identified for IMT in much of Region 1 (EMEA) and eight areas within Region 3 (Asia/Oceania). In Region 2 (including the US) the band has a Primary allocation for Fixed, Fixed Satellite and Mobile services and a Secondary allocation for Radio Location Services (RLS).

On a US national basis, the 3.5 to 3.65 GHz band is historically allocated to RLS and the ground-based Aeronautical Radio Navigation Service (ARNS) on a primary basis for federal use and on a secondary basis to federal non-military RLS usage. The 3.60 to 3.65 GHz band was additionally allocated to Fixed Satellite Service (FSS) earth stations.






	Department of Defense (DoD) Radars	This is in the 3.5-3.65GHz range and includes shipborne Navy radars, ground based radar and systems for weapons control and for air & surface target detection & tracking. The US Navy uses the band for a major radar system on guided missile cruisers and the US Army for a firefinder system to detect enemy projectiles. The US Air Force uses the band for airborne station keeping equipment throughout the US and to assist in possessions for formation flying and drop-zone training.
	Fixed Satellite Services	This is in the 3.6-3.65GHz range, comprising non-federal fixed satellite earth stations and receive-only space-to-earth operations and feeder links. FSS earth stations are licensed in 32 cities in 3.625-3.65GHz plus two earth stations for mobile satellite near Los Angeles and New York City.
	Non-federal Radiolocation	There are three non-federal RLS licences for fixed and mobile RLS in 3.3-3.5GHz and 3.5-3.65GHz.
	Other Uses	There are ship stations more than 44 miles from shore and nationwide fixed broadband equipment in 3.65-3.7GHz.
	Adjacent Services Which May Require Protection	These include high-powered ground and airborne military radars (3.1-3.5GHz) such as systems used on ships and amateur radio.

Illustration 21: Incumbent Uses in the U.S. 3.5 GHz band

Key incumbents and their use in the U.S. 3.5 GHz band is shown in Illustration 21.⁷

⁷ Image Source: GSM Association, *The Impact of Licensed Shared Use of Spectrum*, Deloitte and Real Wireless research, Page 51, Table 3

Key Bridge SAS Infrastructure implements three-tiered spectrum access policies for users operating in the 3.5 GHz band. Through a SAS Infrastructure federal incumbent users are protected; Priority Access Licensee (PAL) users are enabled and protected from harmful interference in their authorized spectrum; and General Authorized Access (GAA) users are enabled to the fullest extent possible without causing interference to higher tier users.

In the 3.5 GHz band there are expected to be two types of federal incumbent user (IU) that may be identified by how information about their use is learned and conveyed to a SAS. These types are *informing* and *non-informing*.

- A **informing federal incumbent user** (IU) is one who proactively notifies a SAS of its spectrum use. Notification may be dynamic, (i.e. via a messaging strategy) or static (i.e. via registration with a SAS or with the FCC).
- A **non-informing federal incumbent user** (NIIU) is one who does not notify a SAS of its use and who's use must instead be separately discerned and detected. In the 3.5 GHz band the discernment and detection responsibilities are assigned to an external Environmental Sensing Capability.

In the 3.5 GHz band all federal IU are co-equal. That is: from the perspective of a SAS one federal user enjoys no priority over another federal user and a SAS provides no de-confliction or coordination service to federal users.

In this regard Key Bridge SAS Infrastructure is a *policy engine* that affords equal, primary protection status to all federal IUs (which includes all NIIUs). IU protections are generally geographically defined. That is, co-channel operation is protected across a defined geographic contour. In the event that the protections afforded of one federal user overlap the protections afforded another federal user the two protections are effectively combined and their union is presented to lower-tier users.

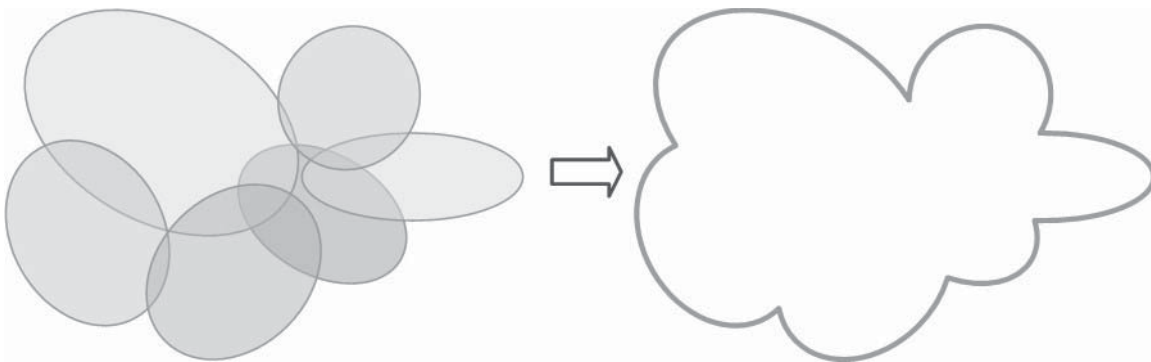


Illustration 22: Incumbent protections are indistinguishably accumulative.

This concept is shown in Illustration 22 and demonstrates how in the Key Bridge SAS Infrastructure federal incumbent protections are *indistinguishably accumulative*.

6.6.1 Informing Incumbent User

Incumbent users will be protected from receiving interference through the use of geographic protection zones as calculated from the details of their registration in the SAS. Registration records may be directly entered via a *SAS Registration Portal* or learned directly from the FCC.

A *SAS Registration Portal* capability for informing federal incumbent users will be developed should such a user class emerge and request service. A mock-up screen-shot SAS Registration Portal for informing incumbent users is shown in Illustration 23. The portal will also include accommodations for users to report complaints or concerns of interference with the SAS.

The screenshot shows a web interface for the Key Bridge SAS Registration Portal. At the top is a dark header with the 'keybridge' logo. Below it is a navigation bar with a home icon and a 'Register' link. The main heading is 'Register and Protect'. The primary section is 'Operating Location', which includes a 'Format' dropdown set to 'Q', a 'Latitude' input field containing '40.759000', a 'Type' dropdown set to 'O', and a 'Longitude' input field containing '-073.979000'. A small instruction 'Click [Type] to extend.' is visible. To the right of the form is a map of New York City, specifically the area around Rockefeller Center, with a red pin indicating the location. The map shows various landmarks like Radio City Box Office, Anthropologie, and Rockefeller Center. The map data is attributed to Google, 2016.

Illustration 23: Incumbent registration portal.

SAS Nodes record informing IU information in their local databases and use this information in their general spectrum availability calculation processes.

Informing IU protections are considered to be static, in that their configuration does not quickly or often change. This does not mean that informing IU protections may not be rapidly effected but rather that their protection is incorporated into the baseline spectrum availability information. New registrations or registration modifications that update spectrum availability may be rapidly propagated throughout a SAS Infrastructure and their impact on spectrum availability conveyed to subscribing CBRS devices.

The 3.5 GHz band does not at present include a *federal* informing incumbent user. Nevertheless, Key Bridge SAS Infrastructure can readily accommodate a informing user type should one emerge in the future by extending the protection procedures and mechanisms used to protect (informing) non-federal incumbent users.

6.6.2 Non-Informing Incumbent User

In the 3.5 GHz band the responsibility to protect all federal incumbent users is assigned to a SAS and responsibility to discern and detect the presence or absence of a non-informing federal incumbent user is assigned to a *Environment Sensing Capability* (ESC). Non-Informing Incumbent Users (NIIU) will be protected from receiving interference through the use of geographic protection zones as specified by the responsible ESC.

NIIU are protected according to the following basic logical decision tree:

- When a ESC is not present:
 - CBSD operation is not authorized by the SAS within Exclusion Zones.
- When a ESC is present:
 - CBSD operation is authorized by the SAS within Protection Zones if allowed by the ESC.
 - Protection Zones are geographic regions defined by the ESC.

In the Key Bridge SAS Infrastructure all federal NIIU are actively protected by default unless and until their absence is positively confirmed by a ESC, in accordance with Commission rules. A ESC description is provided separately in the *Key Bridge Proposal to Administer a Environmental Sensing Capability*. For the purposes of this proposal it may be presumed that a ESC, acting independently and autonomously to the SAS Infrastructure, notifies the SAS Infrastructure of the presence or absence of a non-informing federal IU.

6.7 Protecting Non-Federal Incumbent Users

Non-Federal incumbent users such as fixed satellite service (FSS) earth stations and grandfathered wireless broadband licensees will be protected from receiving interference through the use of geographic protection zones as calculated from the details of their registration in the SAS.

FSS earth station geographic protection zones (colloquially called “contours”) will be calculated by the SAS based upon the station antenna and transmitter configuration. The details and methodology of how FSS contours are calculated is the subject of ongoing work by multi-stakeholder groups in which Key Bridge is a participant.^{8,9}

Non-federal incumbent user information may be learned by a SAS from one of three sources via:

- a ETL data import process from FCC databases; or
- directly from the user via a registration process; or
- peering exchange with another SAS that operates its own registration capability.

Non-Federal incumbent users may register directly with SAS Infrastructure via a (to-be-developed) *SAS Registration Portal* capability, similar to the process described for informing federal incumbent users in 6.6.1 (Informing Incumbent User) and following current practice for incumbent user registration in the Key Bridge TV white space database system.

A 3.5 GHz *SAS Registration Portal* for non-federal incumbent users will be developed in cooperation with end-users to ensure completeness, convenience and continuity of operation. A mock-up incumbent registration portal concept was previously shown in Illustration 23.

The portal will include accommodations for non-federal incumbent users to report complaints or concerns of interference.

⁸ The Wireless Innovation Forum, Spectrum Sharing Committee

⁹ The Wireless Innovation Forum, Reply Comments to GN Docket No. 12-354 , August 13, 2015 at <http://apps.fcc.gov/ecfs/document/view?id=60001121657>

6.8 SAS Priority Access User Services

Key Bridge proposes to use strategies described in the IEEE 1900.5.2 specification to protect priority access (PA) users against receiving interference from general access (GA) users.

IEEE 1900.5.2 is the *Draft Standard for Method for Modeling Spectrum Consumption* and describes a generalized method for modeling the consumption of any type of use of RF spectrum.¹⁰

In the Key Bridge SAS Infrastructure each PA license will be assigned to a responsible SAS Node for handling. SAS Nodes then implement coexistence and protection algorithms for each of its assigned PA licenses using IEEE 1900.5.2-defined spectrum consumption models according to the following general strategy;

- **General.** First, a *general spectrum consumption model* is created describing the the PA license, such as its geographic extent, the maximum number of 10 MHz channels assignable, and other factors yet to be determined according to the developments of a multi-stakeholder group. This first spectrum consumption model serves as a baseline for protecting all PA users within the PA licensed geographic region.
- **Detailed.** Second, a *detailed spectrum consumption model* is generated for each PA user operating under the protection of the PA license. This may be a transmitter model, a receiver model, or any combination of multiple transmitter and / receiver models that together create a network, depending upon the radio configuration presented.
- **Aggregate.** Finally, an *aggregate spectrum consumption model* is calculated that incorporates the combined effects of the first (general) model and each second (detailed) model. This final aggregate model is then used by the SAS Infrastructure to calculate compatibility and coexistence with neighboring PA and GA users, who may be represented by their own aggregate or detailed model.

The *aggregate* model may be updated and re-calculated in real-time according to the operating status of each constituent *detailed* model.

The SAS Infrastructure control channel and pilot channel capabilities described earlier provide the underlying resources to exchange, update, activate and deactivate IEEE 1900.5.2 spectrum consumption models and policies. By this method SAS Infrastructure will enable a priority access license holder to comfortably coexist with neighboring, geographically proximate PA licensees and also to receive fair, consistent, predictable and repeatable protection against interference from GA users.

¹⁰ See IEEE Standards Association IEEE 1900.5™ Working Group at <http://standards.ieee.org/develop/project/1900.5.2.html>

6.9 Modeling and Computing Spectrum Coexistence

IEEE 1900.5.2, the *Draft Standard for Method for Modeling Spectrum Consumption*, describes a generalized method for modeling the consumption of any type of use of RF spectrum. The standard defines an analytical framework and data modeling strategy that may be used to express the boundaries of spectrum consumption by any transmitting or receiving device or any combination thereof (i.e. networks and aggregate populations).

Since 2014 Key Bridge has made significant contributions to the IEEE 1900.5.2 working group, with particular interest to use this standard in a 3.5 GHz SAS and ESC.

Spectrum consumption models naturally lend themselves to efficient evaluation and calculation of spectrum coexistence and identification of risks for potential interference between spectrum users. Any conceivable type and configuration of spectrum consumer may be modeled, including transmitters, receivers, fixed stations, mobile stations, terrestrial networks, aerial platforms, continuous carriers, pulsed signals, frequency hopping waveforms, etc.

The current draft standard includes mathematically robust and repeatable computational methods for arbitrating coexistence between and amongst different *transmitter* and *receiver* and *network* or *device population* models. Using IEEE 1900.5.2, CBRS networks and populations of CBSDs may be readily modeled within a SAS Node and coexistence calculations and analysis efficiently executed against the various CBRS models.

6.9.1 Modeling Transmitters

A IEEE 1900.5.2 *transmitter model* describes the extent and strength of the transmitter radio frequency emission over a geographic region. This model defines the transmitter's emission and geographic service or signal coverage area from the transmitter's perspective. An example signal strength (i.e. path loss) plot is shown in Illustration 24, which shows a simplified decrease of signal power versus (radial) distance from the transmitter. The actual modeled path loss is highly configurable, and detailed later in 6.9.3 (Modeling Signal Propagation).

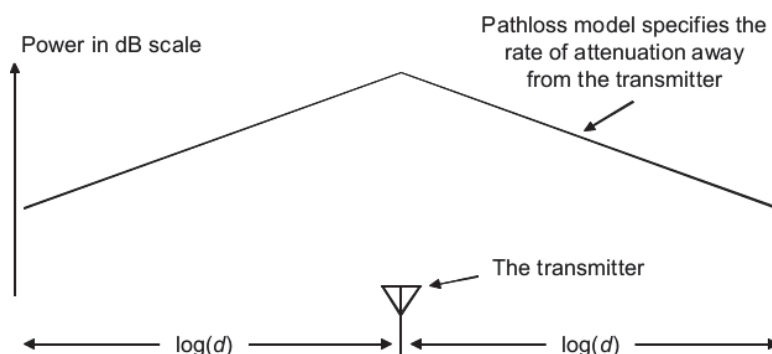


Illustration 24: A modeled transmitter emission.

The transmitter model includes information about the transmitting device's spectral, spatial and

temporal range of use, plus geolocation information to identify where a fixed transmitter may be operated or within which region a mobile transmitter may be expected to operate. Signal levels across a geographic region are projected using a simplified signal propagation model.

6.9.2 Modeling Receivers

A IEEE 1900.5.2 *receiver model* describes the receiver's sensitivity over a geographic region. This model, from the receiver's perspective, defines compatible transmitter configurations or, alternatively, incompatible interference conditions to the receiver. An example sensitivity plot is shown in Illustration 25, which shown increasing sensitivity for locations closer to the receiver.

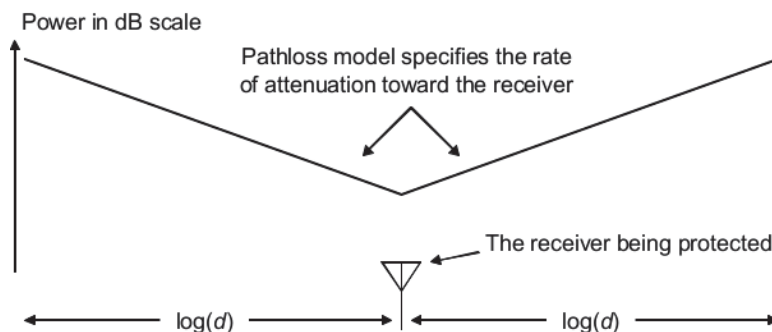


Illustration 25: A modeled receiver sensitivity.

A receiver model identifies a minimum required receive signal power and the location where a fixed receiver may be located or a geographic region where a mobile receiver may be expected to operate, plus a simplified propagation model that other parties may use to establish suitable protection for the describe receiver.

6.9.3 Modeling Signal Propagation

Radio emissions attenuate as they propagate away from their source. The quantity of attenuation is a function of frequency, distance, and the environment. Precise prediction of attenuation is usually a difficult, computationally intensive task and can vary significantly with configuration changes and subtle environmental effects. Examples of commonly used models include ITU-R P.1546, Longley Rice and Okumura-Hata.

The utility of a conventional radio path loss and signal propagation model depends heavily upon an accurate digital elevation model (“DEM”, also commonly referred to as a digital terrain model.) However, large libraries of static raster data are not amenable to use in real-time systems or in distributed applications, and a typical DEM can range from a hundred megabyte to several dozen gigabytes of data. There is therefore great incentive and utility in avoiding SAS dependencies on external terrain model data. The IEEE 1900.5.2 standard handles this complexity and eliminates third-party terrain model dependencies by trading a slight loss of precision with significant simplification and increase in mathematical robustness and repeatability. This is accomplished by modeling signal propagation with a user-configurable

piecewise linear log-distance path loss model. Several example configurations are shown in Illustration 26, where the piecewise linear model parameters are adjusted (by the modeling user) to best match their calculated optimal result for four different configurations. This best-fit matching process can be automated.

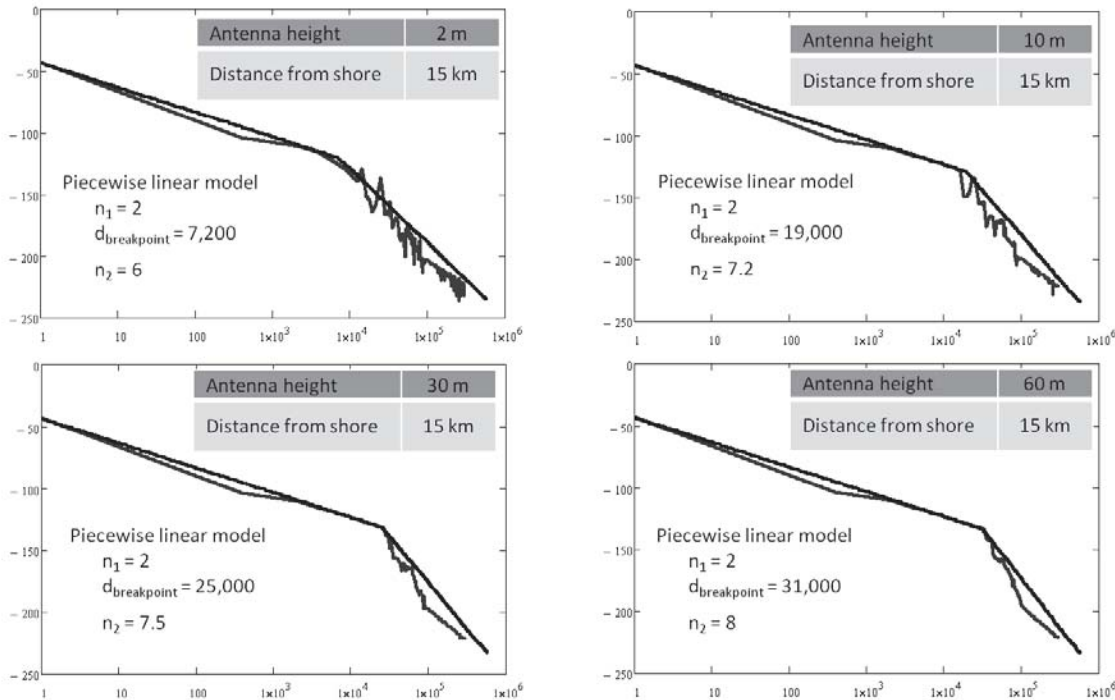


Illustration 26: Modeled signal propagation to match different configurations.

A transmitter signal propagation model, and its inverse: a receiver sensitivity model, describe their expected (or desired for receivers) attenuation of RF emissions versus distance. This attenuation modeled may be radially extended and sectorized to cover a geographic area or region.

The transmitter or receiver model creator (i.e. the transmitter or receiver device owner) may adjust their propagation model to suite, possibly by comparing the modeled propagation with their chosen optimal solution, to achieve the closest acceptable fit for their specific situation. The optimal solution may be any conventional terrain-data dependent path loss model, such as ITU-R P.1546, Longley Rice, Okumura-Hata, etc.

6.9.4 Computing Spectrum Coexistence

IEEE 1900.5.2 spectrum consumption models are readily extended to networks, systems and geographic exclusion or protection zones to evaluate coexistence and to calculate compatible configurations and spectrum use policies for any combination of transmitter and receiver.

The interaction of transmitter and receiver models may be used to determine, generally, whether

the devices are compatible (i.e. may communicate with each other) or the propensity of the two modeled systems to interfere with each other (i.e. may coexist). For example, if the predicted power from a modeled transmitter at the location of a modeled receiver is below the interference threshold established by the receiver then the transmitter – receiver pair may be deemed compatible (i.e. the devices may coexist).

A single transmitter and a single receiver configuration produces a 1900.5.2 computation similar to a classic link budget calculation. The modeled transmitter and receiver combination also provides a power margin that indicates whether and to what extent the receiver will experience interference from the transmitter. Further calculations may determine a maximum allowable transmit power below which the transmitter – receiver pair can reasonably coexist. This is detailed in the IEEE specification and a general representation is shown in Illustration 27.

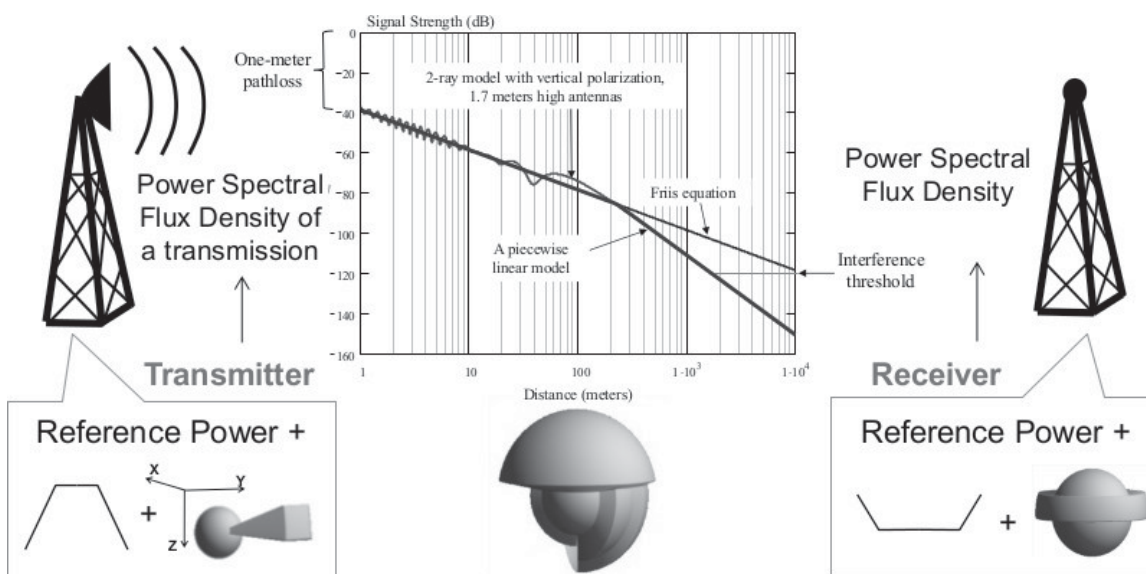


Illustration 27: Assessing compatibility using spectrum consumption models.

The proposed coexistence methodology may be readily extended to collections and networks of transmitters and receivers of arbitrary configuration to approximate and calculate the effect and risk of *aggregate interference*.

IEEE 1900.5.2 spectrum models may be furthermore employed to facilitate coexistence and spectrum sharing by conveying to the modeled transmitters and receivers any required changes to their respective configuration. In the instance of a vertical sharing relationship the conveyed change is for the inferior transmitter to cease operation or to relocate, and in the case of a horizontal sharing relationship a frequency coordination activity could occur.

By employing the IEEE 1900.5.2 modeling strategy a SAS Node, and by extension the SAS Infrastructure, can focus on enabling mathematically robust, repeatable user coexistence without the burden, expense and management overhead of maintaining a large and frequently updated library of digital elevation, terrain and clutter data.

6.10 SAS Administration Operations

SAS Infrastructure is generally configured and administered through a *SAS Administration Portal*. Users may interact with SAS Infrastructure through a *SAS Community Portal*, and devices or other automated systems receive services directly from User Access Service modules configured in their responsive SAS Node.

Key Bridge SAS Infrastructure also has certain external dependencies. Here we discuss how SAS Infrastructure interacts with various external systems to fulfill its service responsibilities.

6.10.1 Records Verification, Correction and Removal

The Key Bridge *SAS Administration Portal* will include capabilities to enable the correction or cause the removal of records by authorized administrators. Key Bridge will employ this capability to respond to any notifications from the Commission or other parties of inaccuracies in the SAS.

Key Bridge will accommodate public inspection, feedback and comment through a *SAS Community Portal*. Key Bridge presently maintains a free public portal to search, review and verify TV-bands White Space records. Key Bridge intends to develop and to provide a similar capability for public search, review and verification of records in the Key Bridge SAS Infrastructure. A screen shot of the Key Bridge Community White Space database and portal is shown in Illustration 28.

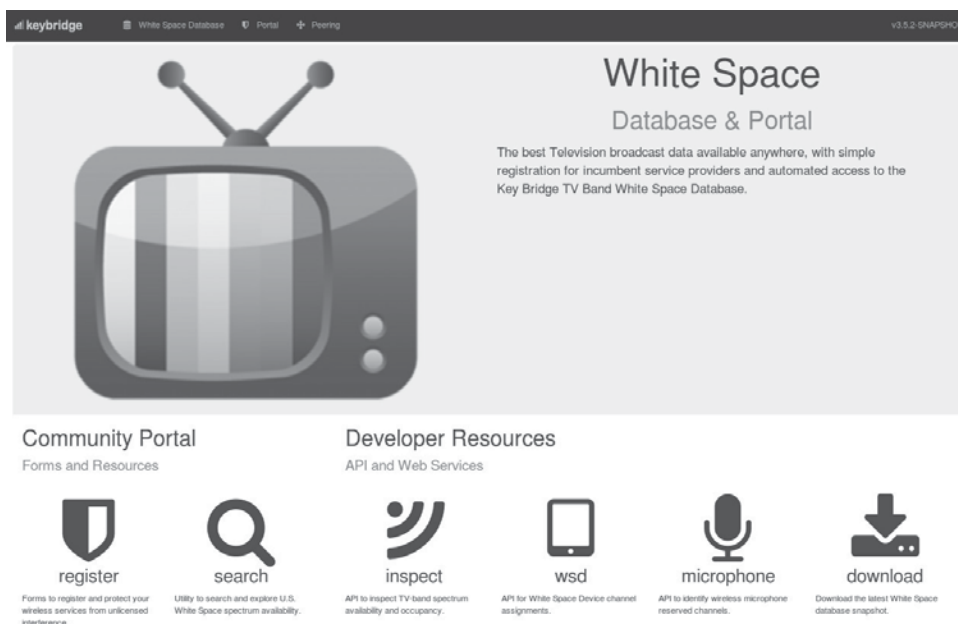


Illustration 28: Key Bridge White Space Portal.

While end users may not edit records in the *SAS Registry Database* they may use the *SAS*

Community Portal to review and identify potential errors, omissions or interference incident reports and to bring such issues to our attention.

In our experience claims of inaccuracies may come in many forms including verbal and written, by telephone, email, etc. To intercept and handle these different forms of input Key Bridge presently operates a ticket tracking system in support of our TV-bands White Space administration. Key Bridge intends to extend this capability to also accept public comment, feedback and notification of any inaccuracies or errors in the Key Bridge SAS Infrastructure.

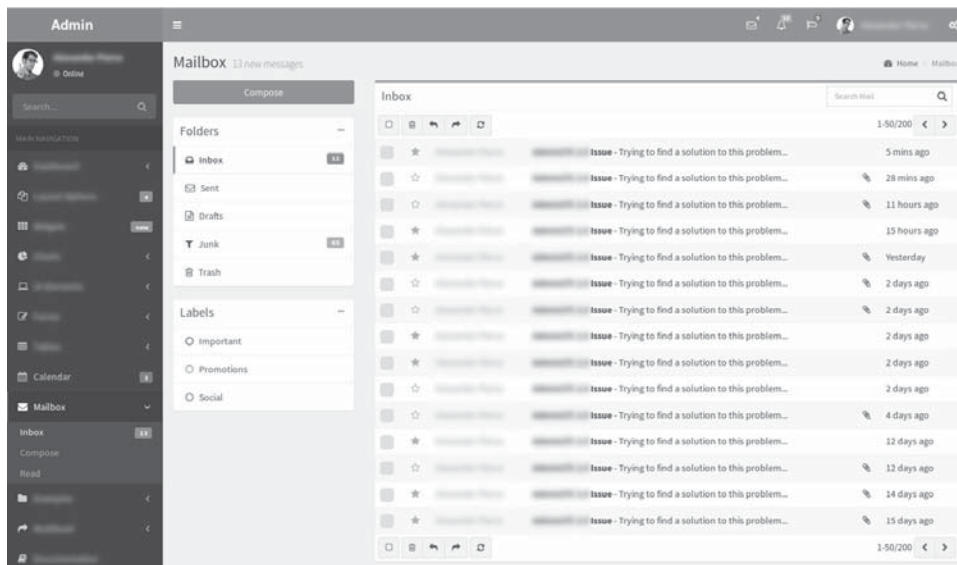


Illustration 29: Example Ticket Tracking System

A mock-up example of the new ticket tracking system under development is shown in Illustration 29.

6.10.2 Interference Incident Reporting and Resolution

To provide full spectrum management capability it is important that all types of significant interference may be reported and expeditiously resolved. All interference has a source (the equipment causing the interference) and a victim (the system or assignment suffering from the interference), and resolving interference between the two may typically be achieved by either readjusting the source or victim parameters and configuration.

It is important to avoid causing further interference effects on other systems while trying to resolve a particular interference,

To the extent possible the SAS will attempt to resolve cases of interference in an automated manner in keeping with the three-tiered access hierarchy in the 3.5 GHz ecosystem. For interference incidents in a horizontal spectrum sharing scenario the SAS will attempt to coordinate automated adjustments between affected devices. For vertical spectrum sharing interference incidents the SAS will implement and enforce spectrum access priorities. Where necessary, the SAS will recruit other responsible SASs via a SAS to SAS peering session.

Where automated resolution is not possible or not adequate t the Key Bridge SAS may escalate interference resolution for manual analysis and intervention. For escalated interference incident reporting, handling and resolution SAS Infrastructure will implement and follow a slightly modified, commercial version of the Joint Spectrum Interference Resolution (JSIR) set of procedures.

In addition to automated escalation from CBSDs, interference incident reports may also be *directly* reported through the *SAS Community Portal*, the *SAS Registration Portal*, or may be *automatically* reported by a third-party operational support system through a *SAS Developer API*. Automated interference incident reporting to the SAS Infrastructure will use the *SSRF Interference Incident Report* (IntfReport) data model, protocol and transaction process defined by the SSRF specification. Interference handling and response procedures will be developed and implemented following guidelines established in the *Joint Spectrum Interference Resolution* (JSIR) procedures. Detailed information about the existing SSRF protocol and JSIR procedures are included in 11 (Appendix: SSRF Interference Incident Report) and 12 (Appendix: Joint Spectrum Interference Resolution)

6.10.3 Geographic Boundary Database

Key Bridge presently offers programmatic access to official geographic boundaries and borders through our GIS suite of applications. Key Bridge *Boundary Web Services* are part of the GIS suite of applications and present a comprehensive database of political, economic and other defined geographic boundaries for reliable presence identification, geo-fencing and other location sensitive applications. A screen shot of the boundary web services API is shown in Illustration 30.

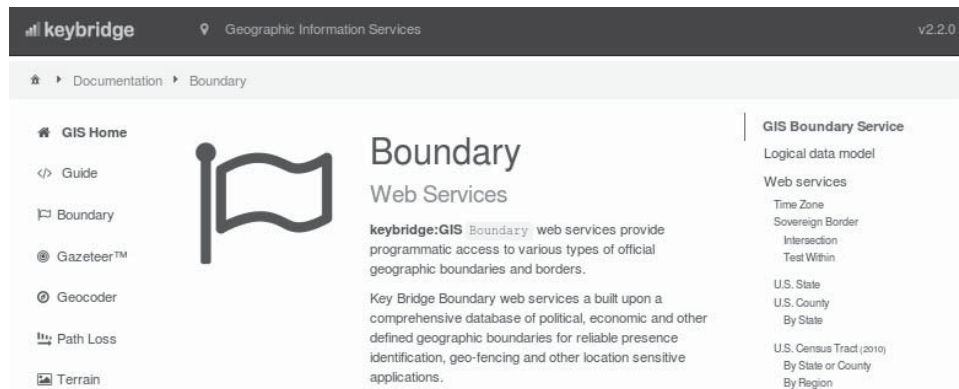


Illustration 30: Boundary Web Services, part of Key Bridge GIS suite

Key Bridge Boundary Web Services include geographic records that describe U.S. political and administrative boundaries including census tracts, various market designations, congressional districts plus city, county, state and national borders.

Key Bridge SAS Infrastructure will retrieve and distribute census tract (PAL) boundaries to SAS Nodes for each respective node's particular configuration from the Key Bridge Boundary web service. NTIA-defined Exclusion Zones and other prescriptive Protection Zone geographic information will be retrieved via similar method.

SAS Infrastructure will retain information on NTIA Exclusion Zones and, when operating with a ESC, ESC-defined Protection Zones in accordance with sections 96.15 and 96.17 of the Commission's rules.

6.10.4 Coordination across International Borders

Arrangements for cross-border coordination are broadly specified in global regulations developed by the ITU-R and in regional regulations developed by organizations such as CITEL. In general, each country has sovereign authority over the spectrum within its borders. Spectrum sharing is essential near international borders where wireless systems can interfere with operations in a neighboring country's territory.

The SAS Infrastructure, through our GIS Boundary service, will be made aware of all relevant geographic borders, territorial boundaries, and exclusion zones that may be negotiated with other countries for coordination of terrestrial wireless and broadcast systems, satellite systems and other technologies. An example mapped boundary of the U.S. Territorial sea and international border with Mexico is shown in Illustration 31. Relevant boundary information for a SAS Node will be configured and downloaded during node provisioning and stored in each respective node's local Data Storage module.



Illustration 31: Plot of the U.S. - Mexico Border and territorial seas.

This approach is similar to our existing, FCC-certified solution for handling international border protections in the TV-band white space.

Spectrum sharing agreements are generally not used for low power opportunistic technologies, such as WiFi, because the impacts of cross border interference are negligible and are typically remedied via self-help when they do occur. This is presently not the case for 3.5 GHz CBRS and SAS Infrastructure will only permit CBSD operations within the sovereign boundaries of the United States.

The Key Bridge SAS solution is flexible and able to quickly implement any future cross-border agreements that may be negotiated between the appropriate national regulatory agencies to coordinate CBRS services in the 3.5 GHz band.

6.10.5 Public Data Exports

The Key Bridge SAS Infrastructure will include a special data export capability to make non-federal, non-proprietary data available to the public. A scheduled process will collect non-federal, non-proprietary records from the *SAS Registry Database* and from *SAS Nodes* in the SAS Infrastructure into a consolidated data set, then make this data available via a public *SAS Developer API*, *SAS Community Portal*, and regularly exported bulk-data file.

Our White Space database system presently implements a similar functionality and we propose to replicate that proven capability.

The period of data collection and export required to preserve operational security and balance public reporting is under consideration in a multi-stakeholder group in which Key Bridge is a participant. This is in progress and not yet determined.

6.10.6 Identifying and Validating Protected Entity Records

Key Bridge provides access to information in our online systems and databases through a collection of web service APIs. This includes public data and information records periodically downloaded or regularly synchronized to the FCC ULS database, a screen shot of which is shown in Illustration 32. See Section 7.1.5 ETL (Extract-Transform-Load) for more information about how our ULS database instance is synchronized to the FCC's ULS database via FCC data file exports.

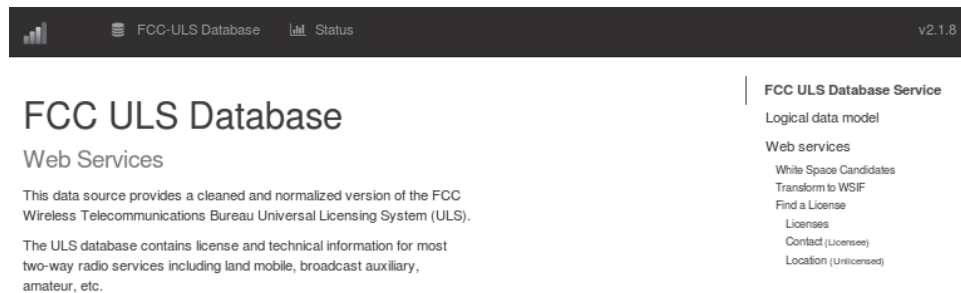


Illustration 32: Key Bridge FCC ULS Database web services portal.

Key Bridge SAS Infrastructure will extract incumbent records from the Key Bridge ULS database via a web service API.

The full FCC ULS database contains million of entries across over 80 different tables. ULS data must be filtered to identify the current, active records that must be protected. There are three record status possibilities for entity classes held in ULS:

- Active
- Unknown
- Pending Legal Status

By default, only records with “Active” status are protected by the SAS.

Transmitting electronic devices, and specifically CBSDs, are required to meet certain FCC technical requirements before they can legally be imported or sold in the USA. Devices are assigned, and may display, an FCC ID number when it has received an FCC grant of Equipment Authorization. The FCC ID consists of two elements:

- a grantee code; and
- an equipment product code.

FCC's Office of Engineering and Technology (OET) is responsible for the authorization of radio devices and provides an interactive search capability to the Equipment Authorization System (EAS) database where users may execute searches based on various parameters including Grantee Code and Product Code. The user form and sample response page are shown in Illustration 33.

FCC Online Communications Commission		Search/SIS Variables (E-Filing Information) Comments (N/A)		FCC Online Data Entry	
Office of Engineering and Technology					
SIS - SIS & SIS - SIS - Automation Search					
Filing Options					
Application Information:					
Grantee Code: [] (press one or three characters of FCCID)					
Product Code: [] Exact Match <input type="checkbox"/> (eliminating characters of FCCID)					
Applicant Name: []					
First Action Date Range (mm/dd/yyyy): [] To []					
Grant Comments: []					
Application Purpose: []					
Software Definition Radio: []					
FAC Assessment Application Only: []					
TCR Assessment Application Only: []					
Comments Application Only: []					
Grant Notes: [] < [] > [] View Grant Note Descriptions					
Set Form: []					
Application Status: All Granted Stations []					
Miscellaneous					
Equipment Class: []					
Frequency Range in MHz: [] To [] Exact Match <input checked="" type="checkbox"/>					
Secondary Bandwidth: []					
Emission Designator: []					
Frequency Tolerance: [] To [] Exact Match <input checked="" type="checkbox"/>					
Power Output in dBm: [] To [] Exact Match <input checked="" type="checkbox"/>					
Bulk Parts Up to (MHz): [] < [] > [] Exact Match <input checked="" type="checkbox"/>					
Product Description: []					
Module Type: []					
Single Modular Approval Limited Single Modular Approval Split Modular Approval OR show all modular OR show all non-modular					
TCR Information:					
TCR Name: []					
TCR Scope: []					
Formatting Options:					
Show results in HTML [] format					
Show [] Records at a Time (HTML output only)					
[Search] [Clear]					

➔

FCC Online Communications Commission		Search/SIS Variables (E-Filing Information) Comments (N/A)		FCC Online Data Entry	
Office of Engineering and Technology					
SIS - SIS & SIS - SIS - Search					
Filing Options					
Application Information:					
Grantee Code: [] (press one or three characters of FCCID)					
Product Code: [] Exact Match <input type="checkbox"/> (eliminating characters of FCCID)					
Applicant Name: []					
First Action Date Range (mm/dd/yyyy): [] To []					
Grant Comments: []					
Application Purpose: []					
Software Definition Radio: []					
FAC Assessment Application Only: []					
TCR Assessment Application Only: []					
Comments Application Only: []					
Grant Notes: [] < [] > [] View Grant Note Descriptions					
Set Form: []					
Application Status: All Granted Stations []					
Miscellaneous					
Equipment Class: []					
Frequency Range in MHz: [] To [] Exact Match <input checked="" type="checkbox"/>					
Secondary Bandwidth: []					
Emission Designator: []					
Frequency Tolerance: [] To [] Exact Match <input checked="" type="checkbox"/>					
Power Output in dBm: [] To [] Exact Match <input checked="" type="checkbox"/>					
Bulk Parts Up to (MHz): [] < [] > [] Exact Match <input checked="" type="checkbox"/>					
Product Description: []					
Module Type: []					
Single Modular Approval Limited Single Modular Approval Split Modular Approval OR show all modular OR show all non-modular					
TCR Information:					
TCR Name: []					
TCR Scope: []					
Formatting Options:					
Show results in HTML [] format					
Show [] Records at a Time (HTML output only)					
[Search] [Clear]					

130 results were found that match the search criteria:
Application Status: All Granted Code and First Action Date From: 01/01/2014 Until: Action Date To: 12/31/2014

Displaying records 1 through 10 of 130.

View	Details	Thumbnail	Applicant	Address	City	State	Country	GR	File No.	Applicant	Final	Inter	Owner
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	12/06/2014		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	06/05/2015	2440.0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	06/05/2015	2442.0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	06/05/2015	2442.0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	06/05/2015	2442.0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	06/05/2015	2442.0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	06/05/2015	2442.0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	06/05/2015	2442.0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	06/05/2015	2442.0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Quantum Systems, Inc.	1700 Alameda, Suite 100	Berkeley	CA	United States	05110	PFD-QC-00000000000000000000	Original Equipment	06/05/2015	2442.0	

[Show Next 10 Rows]
Perform Search Again

Please use the Submit Inquiry link at [www.fcc.gov/oet](#) to send any comments or suggestions for this site

Federal Communications Commission 445 John Street, SW Washington, DC 20554 More FCC Contact Information
--

Illustration 33: FCC Equipment Authorization search form and response.

Key Bridge developed and has successfully operated since 2010 a software module to automate

machine-to-machine confirmation of device certification status by directly interfacing with the FCC's Equipment Authorization System web portal. The Key Bridge equipment authorization verification software interfaces directly with the FCC's own Equipment Authorization search form.

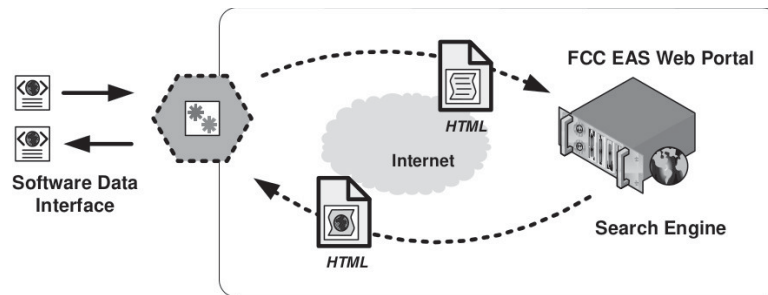


Illustration 34: Automated EAS query.

Key Bridge equipment authorization validation is shown in Illustration 34 and provides an automated, machine-readable resource to

- confirm in real-time and based upon FCC ID that an inquiring device is FCC certified; and
- validate that the device is authorized to transmit on 3.5 GHz bands frequencies.

Device certification data is stored in the SAS Registry Database to minimize processing load on FCC servers. Only one inquiry is required per FCC ID number.

6.10.8 PAL Protection Areas

CBSDs providing service on a Priority Access basis will be protected against interference from other CBSDs – whether Priority Access or GAA – on the same channel in geographic areas and at maximum power levels that will cause aggregate interference in excess of -80 dBm/10 MHz channel within a PAL Protection Area.

PAL Protection Areas will be automatically calculated, persisted and dynamically updated in the SAS Node serving the Priority Access CBSDs and coordinated with other responsible SAS Nodes and external SAS instances via peering.

In addition to SAS calculated PAL Protection Areas, Priority Access users may also self-report their PAL Protection Area using the SAS Registration Portal, which will include a module developed to enable this capability.

Key Bridge has extensive experience manipulating geo-spatial contours and performing sophisticated calculations on geo-spatial contour information. An example of the interactions and intersection relationships between the various default, calculated and reported contours plus their effect in realizing a PAL Protection Area is shown in Illustration 35.

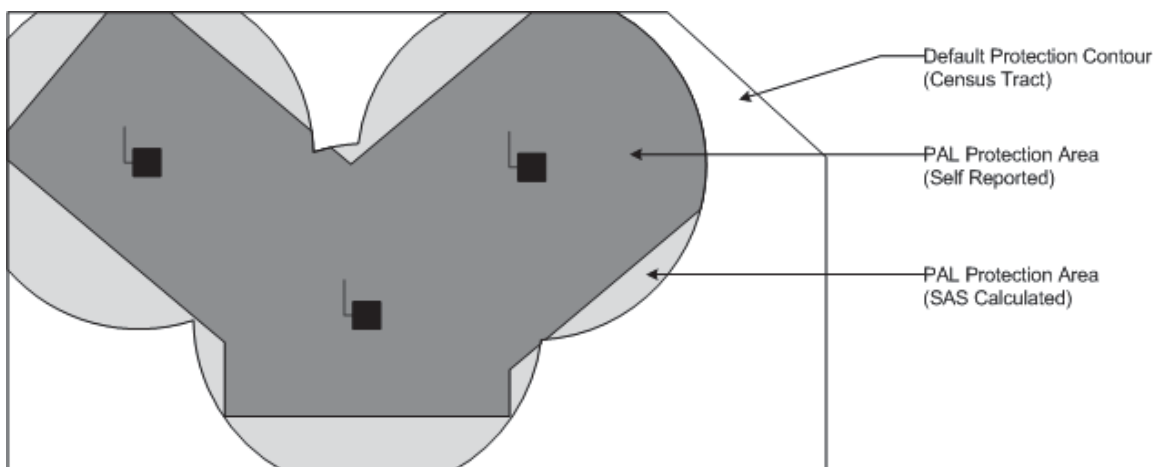


Illustration 35: SAS Nodes evaluate PAL Protection Area contours in real-time.

The aggregate co-channel interference level will be calculated with a common, standardized signal propagation and path loss model and utilizing common inputs and assumptions. Development of a standardized model is already under discussion by a multi-stakeholder group in which Key Bridge participates. Any developed models, inputs, and assumptions – including the propagation model and any clutter or terrain assumptions – implemented in the Key Bridge SAS Infrastructure will be made available for public inspection and review.

7 Key Bridge SAS Functional Architecture

Key Bridge SAS Infrastructure, which is comprised of various SAS Nodes each having a local configuration, provides all of the functions and capabilities identified in the high-level, notional multi-stakeholder SAS architecture previously shown in Illustration 6 and repeated below in Illustration 36.

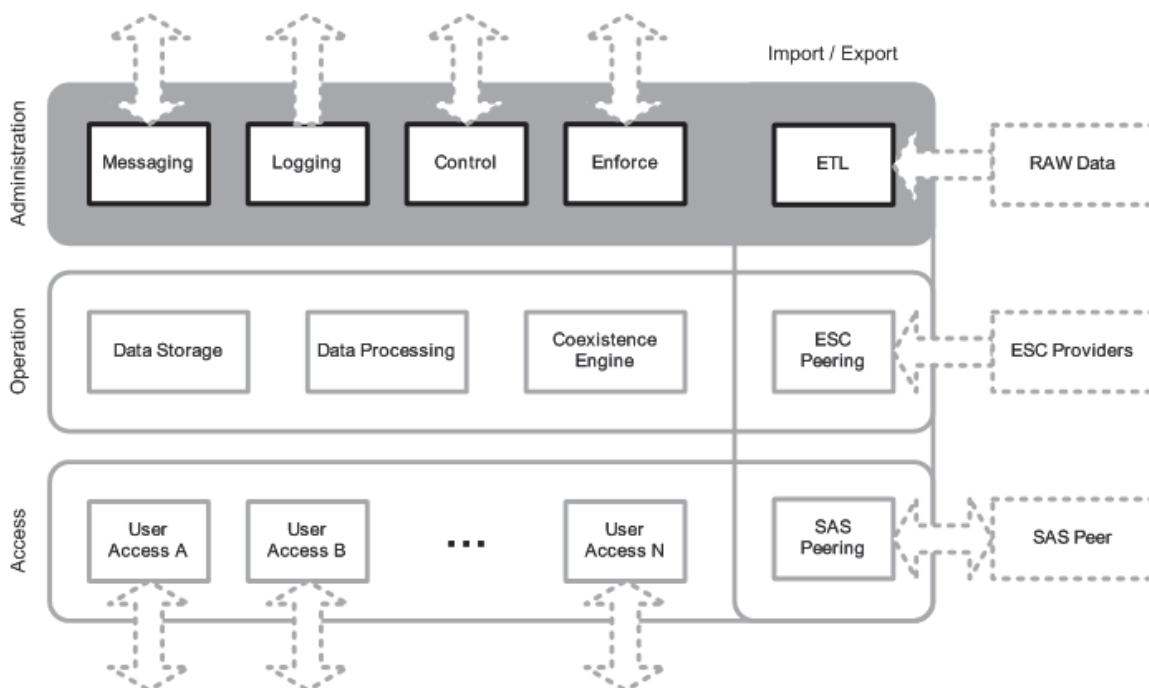


Illustration 36: SAS Node administrative components for management and control.

In a Key Bridge SAS Infrastructure however the various modules, interfaces and software components of any specific SAS Node may be enabled or disabled depending upon that node's assigned role in the SAS Infrastructure and its particular required functionality. For example, in a SAS Infrastructure only one SAS Node need implement a Extract-Transform-Load (ETL) process to import raw data from the Commission. Once imported that information may be distributed to other SAS Nodes via SAS to SAS data exchange.

This concept of distributed functionality is applicable to most aspects of SAS Infrastructure operation including: SAS peering, ESC peering, enforcement, control, etc. In each case a particular SAS Node instance may be designated with a specific role and, in the given examples, act as a primary provider for the indicated function or functionality. This is consistent with the concept of Network Function Virtualization (NFV), where different aspects of an application are developed and tasked separately and bound together via an internal messaging strategy.

7.1 SAS Administration Components

SAS Nodes and, by extension, SAS Infrastructure, are administered through a set of defined management and control applications. This set of software modules, as envisioned in the multi-stakeholder SAS concept architecture, are shown in Illustration 37 and include at minimum: *messaging, logging, control, enforcement* and *ETL*.

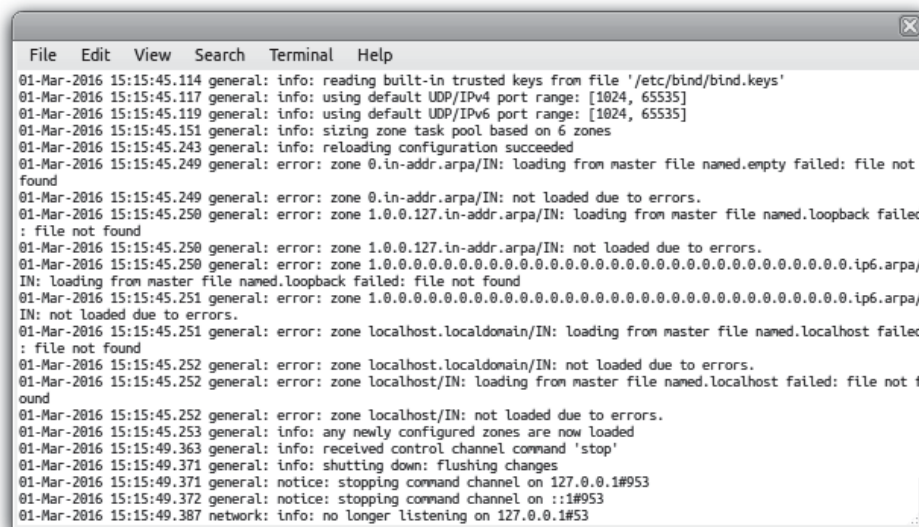


Illustration 37: Example system log contents.

SAS Administration modules may support duplex or simplex communication interfaces plus data exchange depending upon their respectively defined functionality and may generally be accessed via a API. In some instances SAS Administration communication interfaces may also be configured to support local or remote access via a console with command-line interface.

7.1.1 Two-Way Messaging

SAS Administration *Messaging* is a two-way communications software module through which a SAS Node exchanges administrative and status information with other SAS Nodes and with a SAS Administration Portal.

SAS Administration Messaging supports synchronous (i.e. real-time) and asynchronous (i.e. buffered or cached) data exchange. Examples for the use of SAS Node messaging include receiving administrative information requests, forwarding system status updates, operating events and alarms, control and pilot channel routing, etc.

7.1.2 Logging

SAS Administration *Logging* provides a one-way message publication service through which a SAS Node may export information for remote handling (i.e. processing, analysis, persistence, etc.), as opposed to local recording, various system status, event and activity notifications concerning its operation.

SAS Nodes are by default configured to record most system activities and events in log files on the local file system. For example a *system log* maintains a history of system access and operating activities while an *access log* records which administrative users accessed the node and what commands they executed. As an illustrative example, contents of a (Linux) system log file with normal detail is shown in Illustration 39.

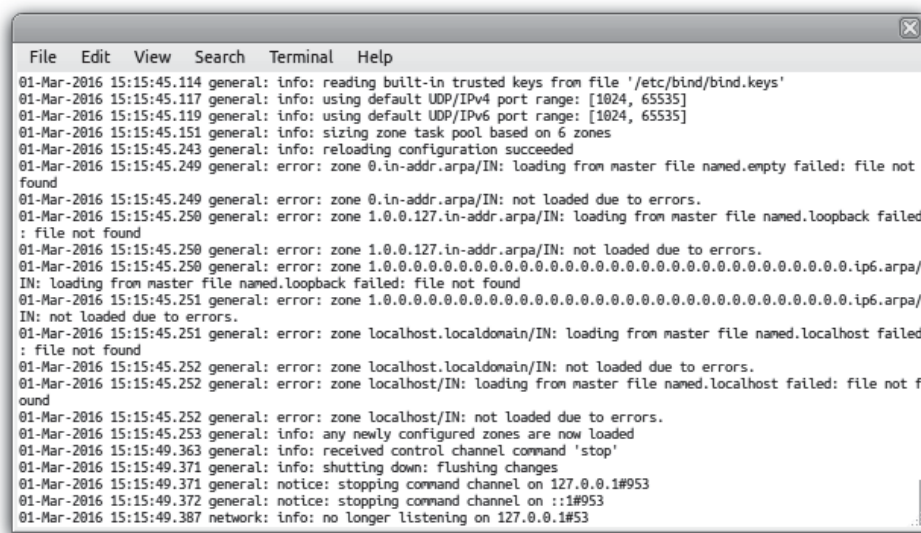


Illustration 38: Example system log contents.

Some or all system activities and events may be additionally or alternatively forwarded to an external logging system for processing and persistence. This is done through the SAS Administration Logging module. Different levels of logging detail may be configured for the various systems and subsystems of a SAS Node depending upon the immediate task and requirements. For example, during commissioning and initial testing a SAS Node may be configured to export tremendously detailed logging information, whereas later, after the node is accepted and placed into production, the logging level may be reduced to only export normal updates, events and alarms.

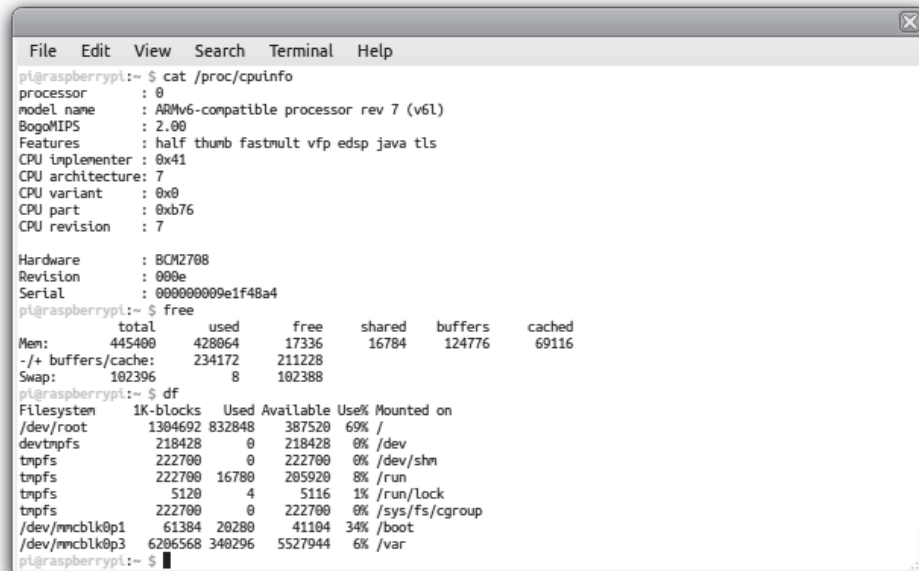
SAS Node logging is a near real-time process, where system activity and event messages are stored locally and/or forwarded immediately after the causative activity occurs or is detected by the node.

7.1.3 Command, Control and Configuration

SAS Administration *Control* enables a SAS Node to be remotely commanded and its configuration modified. SAS Nodes generally support two types of access: automated machine-to-machine access via a proprietary control plane API and direct user access via a *interactive console*.

A SAS Node API facilitates automated remote command, control and system configuration typically via secure communication with a SAS Administration Portal and operations management system.

Authorized users may also directly access, command, control and configure individual SAS Nodes through an interactive console with command-line functionality. As an illustrative example, output from a (Linux) command-line session is shown in Illustration 40.



```

pi@raspberrypi:~ $ cat /proc/cpuinfo
processor       : 0
model name     : ARMv6-compatible processor rev 7 (v6l)
BogoMIPS      : 2.00
Features      : half thumb fastmult vfp edsp java tls
CPU implementer : 0x41
CPU architecture: 7
CPU variant   : 0x0
CPU part      : 0xb76
CPU revision  : 7

Hardware      : BCM2708
Revision      : 000e
Serial        : 000000009e1f48a4
pi@raspberrypi:~ $ free
              total        used        free      shared    buffers     cached
Mem:         445400      428064       17336       16784     124776     69116
-/+ buffers/cache: 234172      211228
Swap:        102396           8       102388
pi@raspberrypi:~ $ df
Filesystem      1K-blocks    Used Available Use% Mounted on
/dev/root       1304692  832848   387520   69% /
devtmpfs        218428      0    218428     0% /dev
tmpfs           222700      0    222700     0% /dev/shm
tmpfs           222700  16780   205920     8% /run
tmpfs            5120      4     5116     1% /run/lock
tmpfs           222700      0    222700     0% /sys/fs/cgroup
/dev/mmcblk0p1    61384   20280    41104   34% /boot
/dev/mmcblk0p3  6206568  340296  5527944     6% /var

```

Illustration 39: Example SAS Node interactive console.

Both the SAS Node control plane API and interactive console enable system interrogation, command and configuration and are cryptographically protected using secure communications protocols and strong counter-party authentication.

7.1.4 Enforcement

SAS Administration *Enforcement* specifically supports and enables supervisory spectrum constraints including geographic, user and device based service limitations. SAS Administration Enforcement receives, processes and prioritizes inbound enforcement instructions.

Key Bridge SAS Infrastructure will support administrative actions described in section 96.63(l) and 96.63(m) of the Commission's rules. While no standardized work flow has been proposed for implementation of these responsibilities Key Bridge will take care to implement such instructions.

The Key Bridge White Space database system includes an administrative capability to implement enforcement instructions from the Commission. A screen shot from the White Space Administration Portal is shown in Illustration 41. Key Bridge intends to replicate this capability in a *SAS Administration Portal*.

keybridge White Space Database Portal Peering v4.1.3

Admin Enforce

FC Enforcement Configure an FCC WSD enforcement action

Use this form to configure an FCC White Space Device (WSD) enforcement action. Enforcements may block channel availability with various degrees of specificity and geographic coverage. An enforcement record requires at minimum one of the following configuration information:
a Device ID, a Device ID & Device SN, or a Geographic Operating Area

Government Authority
Select One
No configured enforcement records.

Registrar
Select a government agency or regulator.

Authorizing Agent
Email Address
Email Address Q
No contact selected.

Device Information
Device ID
Part-15 FCC device ID
Device SN
Device serial number

White Space Device Information
The certifying Part 15 Device ID issued by the FCC and the manufacturer-assigned serial number. The FCC ID number is typically stamped on the device label.

Illustration 40: Key Bridge White Space database enforcement portal.

There are several aspects of operation that enforcement instructions may be expected to address, with the most common being:

- geographic area or region;
- frequency or channel;
- temporal period;
- device class; and

- device identity.

Each of these are accommodated by the SAS Administration Enforcement software module. Enforcement configurations are applied as a cumulative filter and may be combined to establish as much specificity as the Commission may require. For example, the Commission may require SAS Infrastructure to preclude use of a certain channel or channels in a defined geographic area for a specified time and duration. Such a hypothetical requirement may be readily accommodated by the SAS Administration Enforcement software module and, consequently, by the SAS Infrastructure.

7.1.5 ETL (Extract-Transform-Load)

SAS Administration *Extract-Transform-Load* (ETL) imports external data into the SAS Infrastructure. The imported information may be of any type and format and available anywhere on the Internet.

ETL is a standard information management term used to describe a process for the movement and transformation of data. ETL processes are frequently used to populate databases and as enabling capabilities for data migration, data integration and business intelligence functions.

ETL provides normalized data and greatly simplifies programmatic analysis and use; as is shown in Illustration 42.



Illustration 41: ETL provides data normalization.

The three stages of ETL are:

1. **Extract** data of any type from one or more source systems
2. **Transform** the data by applying business rules, cleansing, and validation logic
3. **Load** the results into one or more target systems such as a data warehouse or database

FCC bureaus generally provide technical and licensing database information for public download and use. Most Commission databases are exported nightly into text files between midnight and approximately 4:30 AM Eastern time on the morning after each business day. Exported data files are typically available to the public in compressed archive file format (e.g. ZIP).

Since 2010 Key Bridge has successfully operated a ETL capability that retrieves (i.e. extracts), processes (i.e. transforms) and imports (i.e. loads) data from the FCC's Universal Licensing System (ULS), Consolidated Database System (CDBS), Equipment Authorization System (EA) and International Bureau Filing System (IBFS) into our own local databases.

All records imported from the FCC into Key Bridge database via ETL process are examined, cross-referenced and validated. Any invalid or inconsistent records are identified and logged, and these logs are shared with Commission staff. Over the years the Commission has benefited from this feedback generated by our rigorous data validation processes with thousands of records identified for correction and clean-up.

A new ETL process will be developed to acquire PAL assignments when such information becomes available.

7.2 SAS Operational Components

Internal to a SAS Node are several software operating modules that constitute its core functionality. These essential modules are shown in Illustration 43 and include a *coexistence engine*, a *data processing* module, and a *data storage* (i.e. embedded database) module.

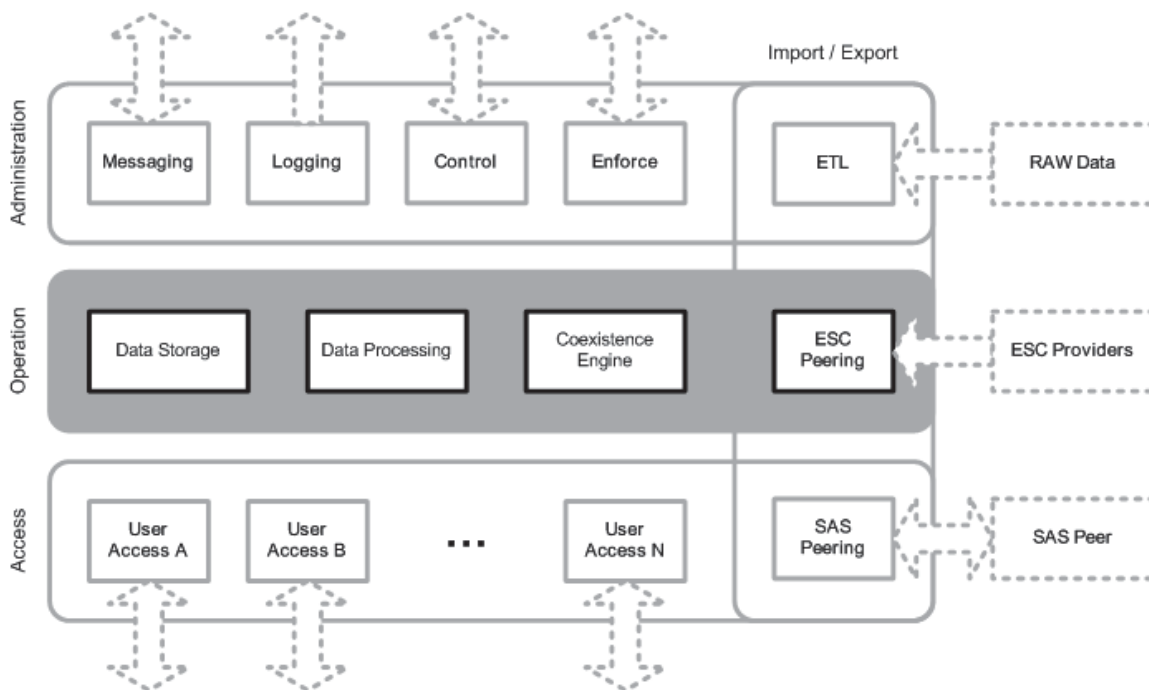


Illustration 42: Operational Components are the core of a SAS Node.

When properly configured and combined into a working system these three components implement the spectrum administration and operating requirements specified in Subpart F of the Commission's rules.

7.2.1 Data Storage

Each SAS Node contains a *Data Storage module*, which is implemented as a local, embedded, relational database containing all records, configurations and other non-transient information necessary for the SAS Node to operate.

Generally only information relevant to or affecting the immediate SAS Node is retained in local data storage. Examples of information persisted in local data storage include PAL contours, exclusion zones, protection zones and other geographic features, records received from other external SASs such as CBSD registrations, FCC-originated records such as FSS and grandfathered wireless service registrations, etc.

7.2.2 Data Processing

A SAS Node *Data Processing* module accepts and processes input requests for spectrum availability. The Data Processing software module reduces and converts such requests to a normalized internal representation, confirms the validity of each request, and supplement or augments the request with information collected from a local Data Storage.

The Data Processing module may be considered in this regard as a message translator. It accepts input requests from various User Access modules, each of which may potentially have a different set of inputs and configurations, and transforms the requests into a normalized (i.e. standardized) internal format that may be forwarded to the Coexistence Engine for handling.

7.2.3 Coexistence Engine

A SAS Node *Coexistence Engine* module is an embedded software application programmed to receive information from various other SAS Node subsystems and to use that information to implement data analysis, perform coexistence calculations and execute other frequency coordination tasks. For example, the Coexistence Engine module is responsible to determine permissible channels or frequencies, power constraints, and other operating configurations for CBSDs at any location within the SAS Node's configuration, such as geo-fenced within a geographic region, operating on a particular channel or set of channels, belonging to a certain class of user, etc.

The Coexistence Engine will attempt to harmonize, coordinate and stabilize spectrum assignments for CBSD users. This includes, wherever feasible, assigning the same channel to PA users operating across geographically contiguous census tracts where the license is held by the same network operator and also attempting to maximize the amount of contiguous spectrum in any given spectrum assignment.

In its simplest form a SAS Node Coexistence Engine accepts input messages from a Data Processing module, combines this input with information from a ESC and other (external) SAS instances, and then performs a set of computational analyses against all available and relevant data including applicable spectrum policies, and calculates a spectrum use configuration.

7.2.4 SAS to ESC Peering

The SAS *ESC Peering* module is an embedded software module that enables secure communication with external Environmental Sensing Capability (ESC) service providers.

SAS to ESC peering operational security policies and configurations are under development within a multi-stakeholder group in which Key Bridge is a participant.¹¹ The actual protocol and data structures for SAS to ESC peering is not the subject of multi-stakeholder group consideration. Key Bridge has therefore invented proprietary and also proposed non-proprietary methods that a SAS may use when coordinating with a ESC to dynamically protect a non-informing incumbent spectrum user.

For SAS to ESC peering Key Bridge has developed and will use a *SAS Gateway Protocol* to establish and maintain information exchange capability between a Key Bridge ESC and SAS. The Key Bridge SAS Gateway Protocol is, at present, a proprietary application peering protocol that includes mechanisms to support cryptographically secure message exchange for both SAS to SAS and SAS to ESC peering, including all security prescriptions identified by the multi-stakeholder group.

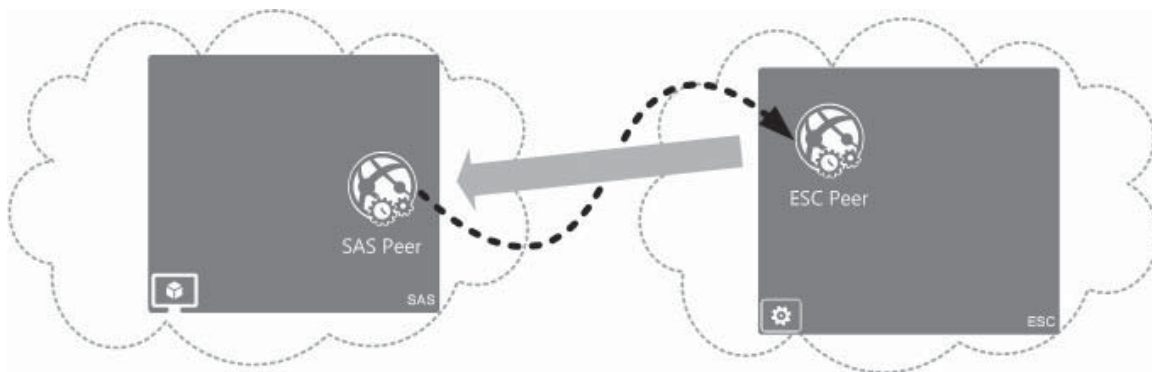


Illustration 43: SAS to ESC Peering masks internal architecture.

A SAS exterior peering protocol standard will place no constraint on the internal architecture and operation of the various entities that use the protocol. This concept is shown in Illustration 44, where a Key Bridge (distributed, networked) SAS Infrastructure on the left peers with a foreign ESC on the right of unknown constitution.

When using the Key Bridge SAS Gateway Protocol a SAS Node, designated by the SAS Infrastructure as a *SAS Peer*, may register with and receive information from a external ESC Peering service. Both the SAS Peer and ESC Peering service implement and exchange messages using the SAS Gateway Protocol.

Using the SAS Gateway Protocol, Key Bridge SAS Node to ESC peering generally involves two steps: *registration* and *operation*, which are indicated in Illustration 44 by the dotted and solid lines, respectively.

¹¹ The Wireless Innovation Forum, Spectrum Sharing Committee, Working Group 2: *Security*.

- **Registration.** SAS to ESC peering begins with a registration process, where a designated SAS Node (called a SAS Peer) registers itself and other SAS Nodes with a ESC. The registration process includes notifying the ESC of SAS Node geographic regions of responsibility and instructions describing how the ESC may query SAS Nodes for additional information.
- **Operation.** Once a peering session is established the ESC forwards spectrum event, occupancy and other required or desired information to each registered SAS Node. ESC messages are securely routed through the SAS Peer.

7.3 SAS Access Components

SAS Access Components provide the communications interfaces through which users and client systems may interact with a SAS Node. This includes any number of *User Access Service* modules, each developed and configured to match the type and configuration of the User Access network or system, and a *SAS Peering* module. SAS Access Component software modules, as envisioned in the multi-stakeholder SAS concept architecture and implemented in a Key Bridge SAS Node, are highlighted in Illustration 45.

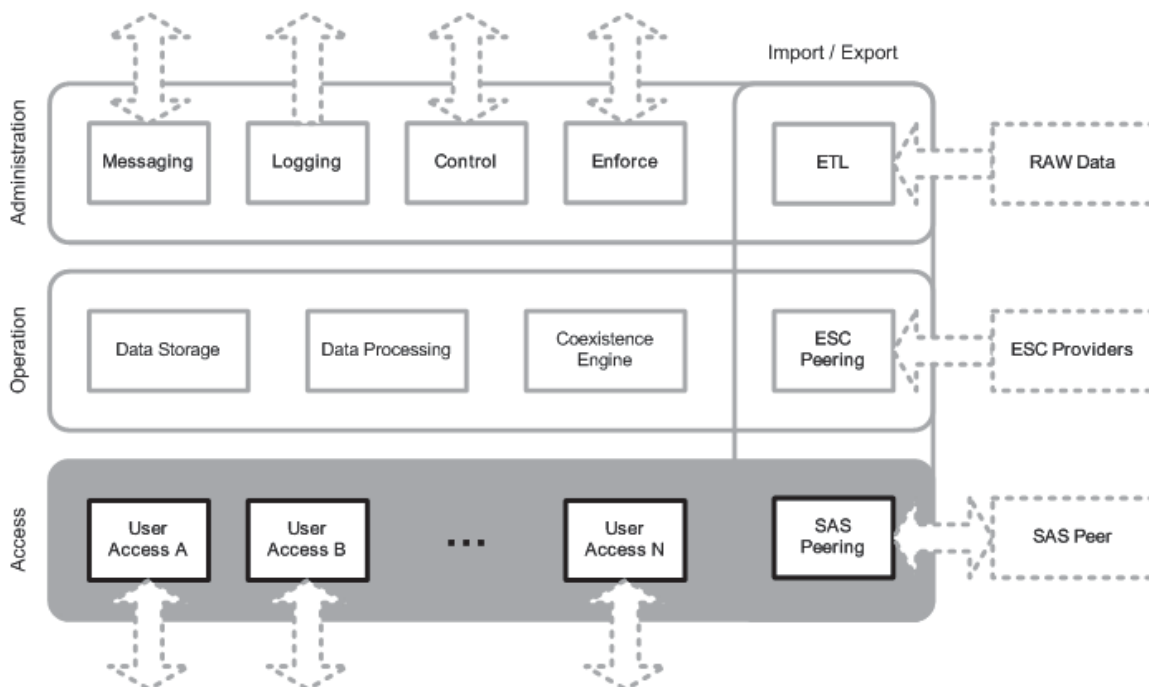


Illustration 44: SAS Node access components provide User Access Services.

SAS Access Components are under active development. The data models and protocols to exchange data with a SAS Node plus the contents of any exchanged messages are still being formulated. Key Bridge is an active participant in this work and chairs a multi-stakeholder group presently developing protocols and associated data formats for SAS User Access Services and SAS to SAS Peering communications.¹²

Accordingly, we present here a high-level description of how a SAS Node is expected to provide spectrum access services to end users through *User Access Service* modules and also exchange information with other SAS instances outside a Key Bridge SAS Infrastructure through a *SAS Peering* module.

It should be noted that an actual configuration that Key Bridge will develop and present to the

¹² The Wireless Innovation Forum, Spectrum Sharing Committee, Working Group 3: *Protocols and Data Formats*. (WG3)

Commission for testing and certification may be substantively different. Regardless of implementation detail however the Key Bridge SAS Infrastructure, its interactions with end users and its exchange with peer SASs will comply with all aspects of the Commission's rules.

7.3.1 User Access Service

SAS Nodes interact and provide spectrum access services to users through one or more *User Access Service* modules. User Access Service modules are developed to match the user access technology and support communication protocols of the end user networks such as LTE, WiMAX, WiFi, etc. User Access Services may necessarily extend those protocols with SAS-specific data elements and to messaging transactions required for 3.5 GHz operation including frequency allocations, channel assignments and other dynamic spectrum sharing capabilities.

Key Bridge envisions that any particular SAS Node instance will typically be configured to interact with and provide User Access Services to one user network type at a time. That is: one SAS Node may be provisioned to interface with LTE users; another provisioned to support WiMAX users, and yet another to support a third network type.

Key Bridge presently chairs a multi-stakeholder group that is working to develop a industry standard framework and protocol for SAS-to-CBSD communications.¹³ This work is in progress, with drafts of the proposed interface and protocol recently published and included herein by reference.¹⁴ Additionally, Key Bridge participates in a separate multi-stakeholder group that is working to develop industry standard communications security framework for SAS-to-CBSD communications.¹⁵ This work is also in progress but not yet published.

According to the SAS-to-CBSD communications protocol under development a CBSD may use static or dynamic methods for SAS discovery and all information exchange is secured using protocol encryption.

13 The Wireless Innovation Forum, WG3

14 The Wireless Innovation Forum, WG3, *Interim SAS to CBSD Protocol Technical Report-A* at <http://groups.winnforum.org/d/do/8699> and *SAS to CBSD Protocol Technical Report-B* at <http://groups.winnforum.org/d/do/9032>

15 The Wireless Innovation Forum, Spectrum Sharing Committee, Working Group 2: *Security*

7.3.2 SAS to SAS Peering

SAS Peering borrows, at a high level, from Internet route peering and database synchronization, where each FCC-designated SAS Infrastructure is considered to be atomic and autonomous, and contains within itself an authoritative capability to provide spectrum access services within its prescribed geographic area of operation.

In the Key Bridge SAS Infrastructure SAS Nodes “peer” with other SAS instances through a SAS Peering module, which provides for the secure, transactional exchange of messages between SASs. Depending upon the context a Peering module may communicate “externally” with another autonomous SAS instance or it may communicate “internally” with other SAS Nodes in the Key Bridge SAS Infrastructure. These two communications methodologies are called *external* and *internal* peering, respectively.

- **External Peering.** In a external peering relationship one SAS exchanges information with another independent, autonomous SASs. Capabilities supported by a external SAS peering session include coordinating operations between and among heterogeneous CBSDs, providing a stable radio frequency environment and other functions required for orderly spectrum administration and the fulfillment by the SAS of the responsibilities given it under Part 96. Key Bridge presently chairs a multi-stakeholder group that is working to develop a industry standard protocol for external SAS to SAS peering.¹⁶ This work is in progress, with drafts of the proposed interface and protocol recently published and included herein by reference.¹⁷
- **Internal Peering.** Key Bridge SAS Nodes route messages using the *SAS Gateway Protocol*, a proprietary protocol developed by Key Bridge for inter-SAS message routing, coordination and cooperation. The Key Bridge SAS Gateway Protocol leverages concepts from other routing gateway protocol and includes mechanisms to support cryptographically secure message exchange for both internal and external system peering. The protocol is generally a superset of the recently published draft external peering protocol and includes certain improvements such as counter-party authentication, message integrity and non-repudiation, managed sessions, stateful transactions, auditing, logging, etc. Ultimately we hope to either merge the two approaches or to propose the SAS Gateway Protocol as the basis for standardized application peering through a capable multi-stakeholder group. As the protocol and its implementation are further perfected Key Bridge intends to release documentation and various open-source implementation examples.

A SAS exterior peering protocol standard will place no constraint on the internal architecture and operation of the various SASs and SAS Infrastructure that use the protocol. For example, one SAS may be a single monolithic Internet application while another is a constellation of SAS

¹⁶ The Wireless Innovation Forum, WG3

¹⁷ The Wireless Innovation Forum, WG3, *Interim SAS to SAS Interface Technical Report-A* at <http://groups.winnforum.org/d/do/8834> and *SAS to SAS Interface Technical Report-A* at <http://groups.winnforum.org/d/do/9036>

Nodes comprising a SAS Infrastructure. This concept is shown in Illustration 46, where a Key Bridge (distributed, networked) SAS Infrastructure on the left peers with a foreign SAS on the right of unknown constitution.



Illustration 45: SAS to SAS Peering masks internal architecture.

Similar to internet routing protocols, the exterior SAS peering protocol ultimately implemented between the various FCC-authorized SASs will enable autonomous SAS Infrastructures to enter and exit a peering relationship at any time, and a new SAS peering session is bootstrapped by the joining party by assembling a complete data snapshot from a “active” system to the “new” system. The SAS peering session is kept synchronized through the regular, bi-directional exchange of updating messages.

The implemented peering protocol will also ensure that all information exchanged in a SAS peering session is cryptographically protected.

8 Key Bridge SAS Security Architecture

The Key Bridge SAS Infrastructure enforces a *positive security model* to prevent unauthorized access, protect sensitive data and limit the effects of a potential breach, attack or failure. In computer security a positive security model is also called as "white list" and defines *a priori* all allowed conditions while rejecting everything else. This contrasts with a negative (i.e. "black list") security model which attempts to identify and filter what is explicitly disallowed while implicitly allowing everything else.

The Key Bridge SAS Infrastructure positive security model employs digital cryptographic certificates and is enforced using *security domains*.

In information security a *security domain* is an enclave of computer applications that are kept separate from other applications. Within a security domain applications are typically configured to trust one another and may freely communicate. In a networked environment different security domains may be created using firewalls to limit communication with other domains. In a cloud-based operating environment security domains can be dynamically established using virtual networks and virtualized firewall configurations.

The Key Bridge ESC Infrastructure security domains are created based upon *functional isolation* and *logical segmentation*.

- **Functional isolation** is a system security technique that groups applications and computer systems with similar functionality and security threats profiles into a dedicated security enclave. It allows the application of tailored security profiles to counter known threats and limit the possible impact of unknown threats.
- **Logical segmentation** supervises resource availability for applications. Logical segmentation creates security communities across system components without regard to their physical location. It creates a flexible, layered security approach based on applications, application groups, IP addresses and geographic regions and allows the creation and application of tailored security profiles to isolated applications and computer systems.

Logical segmentation has several key benefits, principal among them the ability to pinpoint and prevent attacks at a very fine level. It provides a robust method to prevent "pivot" attacks, where one compromised service is exploited to attack others. The Key Bridge SAS security solution has tremendous flexibility in this respect; it accommodates data security at the physical and logical networking layers, in between security enclaves, and between the various service applications.

The distributed architecture of SAS Infrastructure and its use of secure message routing provide inherent compatibility with a functional and a logical partitioning strategies. A SAS Node is the service providing entity within the SAS Infrastructure and is the basic unit around which a logical isolation policy is created. That is: Each SAS Nodes in a SAS Infrastructure is logically isolated into its own security enclave and may only communicate with other SAS Nodes via a peering interface.

This concept of logical segmentation is also more generally applicable. A high level overview of the Key Bridge Infrastructure logical segmentation strategy is presented in Illustration 47 for reference.

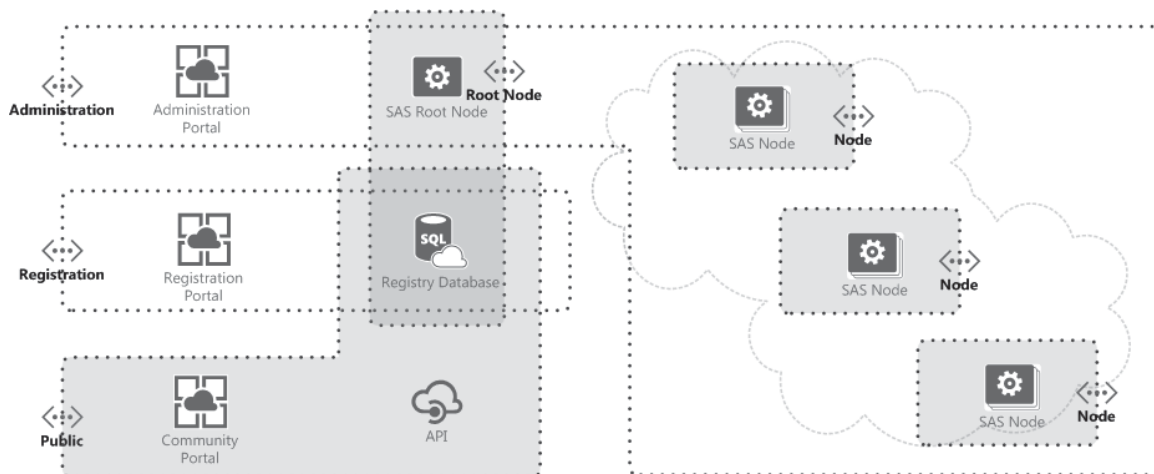


Illustration 46: SAS Infrastructure incorporates layered security domains.

In the Key Bridge SAS Infrastructure different, layered security domains are created to enforce a positive security model for communications between different enclaves.

- **Administration.** An administration security domain provides for global monitoring of system health and performance plus operating configurations and policies.
- **Registration.** A registration security domain allows for informing, non-federal incumbent registration and supplemental data entry.
- **Public.** A public security domain provides access to a centralized *SAS Registry Database* for information query and retrieval.
- **Root Node.** The *SAS Root Node* is a special security enclave with read and write access to the centralized *SAS Registry Database*.
- **Node.** Each SAS Node is a discrete security enclave, and communications between Node enclaves is controlled with a positive communications strategy.

Not labeled in the illustration is a **Database** enclave protecting the centralized *SAS Registry Database* that contains important operational information such as the geographic locations and configuration of protected FSS stations, Exclusion Zones, Protection Zones, plus spectrum availability information, SAS Node geographic assignments, system health and performance metrics, etc.

Internally, a SAS Node is itself a collection of discrete, inter-operating software modules and each communications module within a SAS Node is contained within a local (functionally isolated) security enclave and may only communicate with positively identified and authorized end points via prescribed interfaces. This concept may be further explained by reference to

Illustration 48, where the various North, East and South-bound software modules and communications interfaces are each contained within different security enclaves, each configured according to their function.

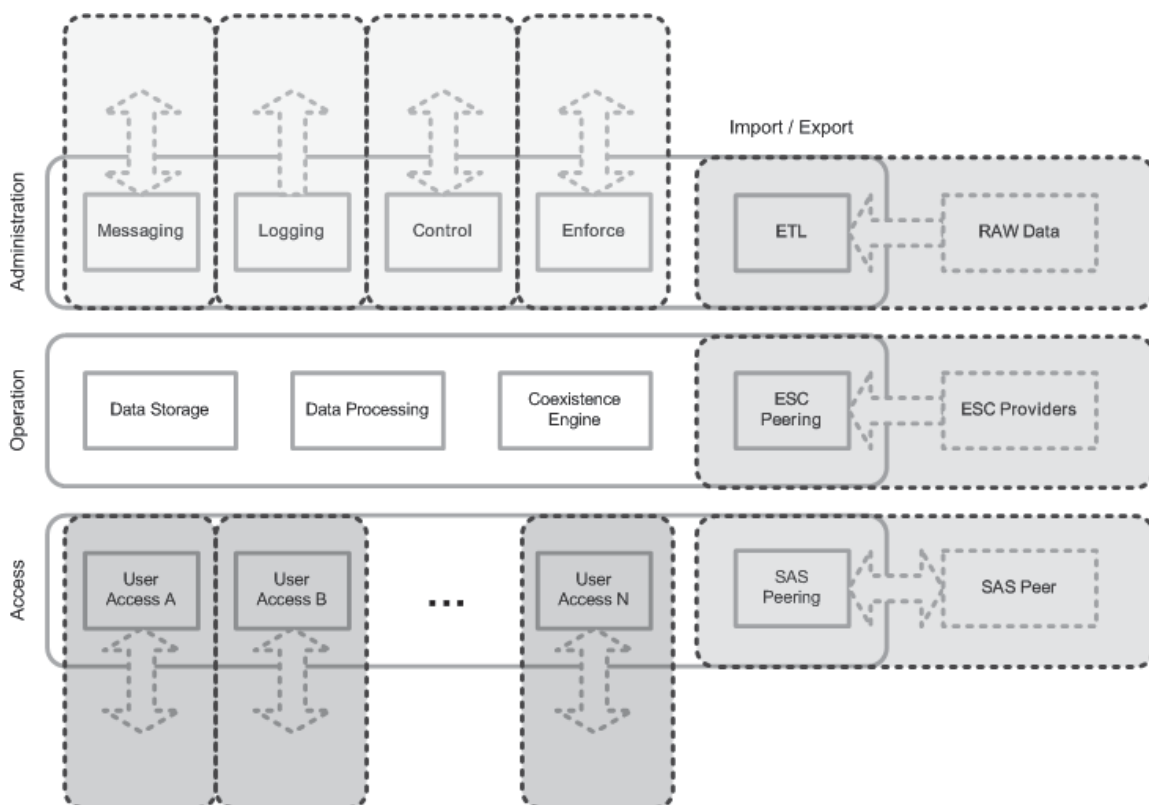


Illustration 47: SAS Node communications are protected by functional security enclaves.

Each connection between enclaves, both logical and functional, in the Key Bridge security architecture represents a policy enforcement point where Key Bridge may enforce granular control of application and message traffic, pinpoint anomalies, and prevent undesired activity either from internal mis-configuration or malicious act.

8.1 Database Security

Key Bridge implements several forms of database security to ensure the integrity and confidentiality of system information. This includes a general prohibition on direct access, record field encryption, plus other industry best practices.

- **Direct Access.** Direct read or write access to a database is not allowed and is disabled (where possible) in production systems. All database access, and specifically all information WRITE operations in the Key Bridge architecture must be processed through software that is carefully developed to include pre and post-persistence data integrity checks, atomic, consistent, isolated and durable (ACID) transactions and logging. This applies for both the centralized SAS Registry Database and for each embedded SAS Node database.
- **Field Encryption.** Sensitive record fields are encrypted prior to persistence in a database. In some instances, such as with user passwords, the original information is not persisted at all. Instead the result of a one-way hash algorithm is persisted in the database. In other instances the original information may be decrypted in software with a user-provided token, key or password. In both cases the original information is protected in the event of a data breach or unauthorized disclosure.

Database security is an important aspect of SAS security and is critical to successful, uninterrupted operation. The Key Bridge security architecture plus our data handling and database implementation strategies mirror those implemented in our TV-bands White Space database system, which have proven effective thus far at managing security and confidentiality of the information entrusted to our care and at minimizing the risk of breach or unauthorized disclosure.

8.2 Communications Security

Messages received from the Internet cannot be trusted by default. The Key Bridge SAS Infrastructure positive security model does not allow connections or communications with unknown parties. The Key Bridge SAS employs several procedures and technologies to implement system security and a positive security model. These include:

- Only authorized SAS Nodes may peer
- All Nodes employ mutual authentication using X.509 certificates
- Insecure communications are not allowed
- All communications between endpoints is protected by Transport Layer Security (TLS) or IPSEC
- Messaged data exchange must employ end-to-end cryptographic protection with authentication, integrity and confidentiality procedures

The SAS Infrastructure is a asynchronous, messaging-based distributed application that incorporates a standards compliant implementation of *Web Services Security* (WS-Security) to enable secure communications across the Internet.

WS-Security is a formally defined is an extension to the *Simple Object Access Protocol* (SOAP) that includes procedures and software protocols for securing Web services. The WS-Security specification describes SOAP messaging enhancements that provide integrity, confidentiality, and mutual authentication for secure data transactions. The WS-Security protocol was originally developed by IBM, Microsoft, and VeriSign and has become a widely adopted open software standard.

WS-Security provides end-to-end transaction security by incorporating security features directly within messages. It specifies how web services may offer integrity and confidentiality, how digital signatures may be attached and encrypted data embedded within messages. The WS-Security specification provides three mechanisms for securing Web services at the message level: *authentication, integrity and confidentiality*.

- **Authentication** uses a *security token* to validate users and determine whether a client may access a web service. Clients can be end users, machines, applications, or other web services. Without authentication, an attacker can use spoofing techniques to send a modified message to the service provider.
- **Integrity** uses message signing to ensure that message data is not changed, altered, or lost. Integrity uses *XML digital signatures* on the contents of messages. Without integrity, an attacker can use tampering techniques to intercept a message between the client and server and then modify it.
- **Confidentiality** uses *message encryption* to ensure that only unauthorized parties with proper access may read message information. Without confidentiality, an attacker can use

eavesdropping techniques to intercept a message and read the contained information.

Key Bridge WS-Security implementations provide robust, standards compliant and proven message security solution that meets the most demanding processing and threat environments.

8.3 Software Security

Key Bridge software is primarily developed in the Java™ programming language and executed in a Java™ virtual machine (i.e. a Java™ platform).

The Java™ platform supports digitally signed application executables, called Java Archive (JAR) files. The ability to sign and verify files is an important part of the Java platform's security architecture. Security is controlled by the security *policy* established and implemented at runtime by the Java virtual machine.

The Java platform enables JAR signing and verification with public and private *keys*, and the X.509 *certificate* that the signer is included in a signed JAR file.

All software in the SAS Infrastructure will be digitally signed. This includes the SAS Administration Portal, which will be built with industry standard Java EE and associated enterprise security technologies.

Other applications such as the various software modules operating within SAS Nodes are expected to be developed as OSGi applications. OSGi is a modular Java operating environment. Securing Java applications running in a OSGi environment is very similar to securing enterprise applications, and for most security frameworks, no additional steps are required. For Java security in enterprise applications, one sets permissions at the application level. For OSGi applications, one may also set security permissions at the bundle (i.e. the JAR) level.

To the extent that embedded Java software is developed and run in a OSGi environment, those applications will be configured with a bundle-level security permission configuration.

8.4 Public Key Infrastructure

The Key Bridge SAS architecture incorporates a Public Key Infrastructure (PKI) each SAS Node may include an embedded Certification Authority (CA) software application to generate, issue, validate and revoke public / private key pairs and X.509 certificates using a brokered authentication strategy.

Brokered authentication with X.509 certificates issued by a certificate authority in a PKI is shown in Illustration 49 and involves the following participants:

- **Certificate authority (CA).** A CA is an authentication broker that is responsible for authenticating clients and issuing valid X.509 certificates. Each SAS Node in the SAS Infrastructure may be configured as a CA.
- **Certificate store.** This is where the X.509 certificates are located. Each SAS Node operating as a CA maintains a local certificate store.
- **Client.** A client accesses service and authenticates itself to the service provider using a X.509 credential. In this context clients may be peer SAS Nodes, CBSDs, or other parties requiring access to various SAS services.
- **Service.** The service is a SAS Node service that requires client authentication and authorization.

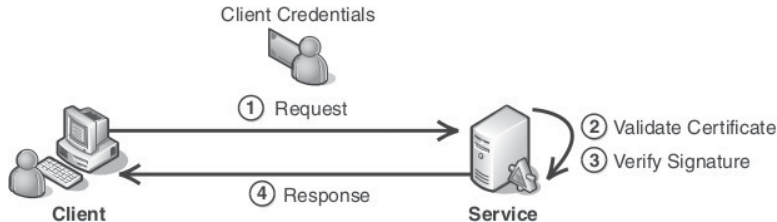


Illustration 48: Authentication using an X.509 certificate.

There are many options available when designing a PKI and the exact configuration of the Key Bridge SAS PKI, whether it should be *hierarchical*, *multi-root*, or *distributed mesh*, for example, remains under development.

Regardless of which architecture is finally adopted in the Key Bridge Infrastructure the PKI configuration will be immune to standard threats such as message insertion, modification, and man-in-the-middle attacks because all information in a end user certificate and used by a CA, including policy mapping and constraints, is digitally signed by another trusted CA, that being either a Root CA or another CA generating a cross-certificate.

8.5 Counter-Party Authentication

Authentication is the process of identifying an individual using the credentials of that individual. There exist a variety of models for counter-party authentication, including *direct authentication*, where a parties establish a bilateral trust relationship, and indirect or *brokered authentication*, where a parties establish a third party trust relationship.

Security and system architecture considerations may support one approach over the other. For example, message protection requirements may dictate the use of brokered authentication when direct authentication is available. The support for different security infrastructures also has an influence on the authentication method used.

SAS Infrastructure employs both direct and brokered authentication for its various functions, where the authentication strategy is applied based upon the context, type of service, and scope of access.

Direct authentication involves the use of *pre-shared secrets* where a client application and a service establish credentials prior to the client using the service. This concept is shown in Illustration 50. Examples of direct authentication include basic passwords and SSL certificates.

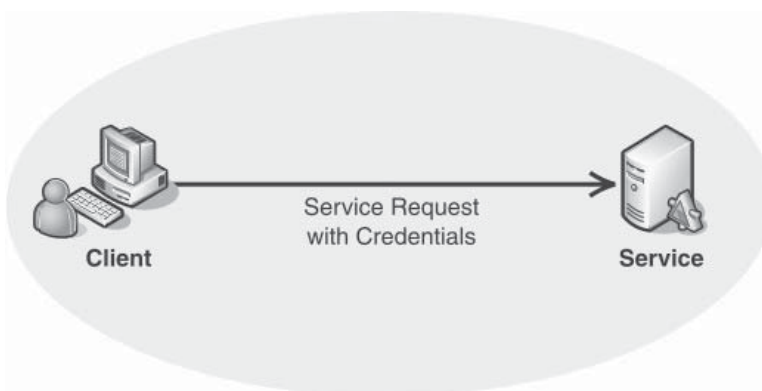


Illustration 49: Direct authentication uses pre-shared secrets in a trust relationship.

SAS Infrastructure uses direct authentication for user access to SAS Portals (with a user name plus password), plus potentially for automated access various consumer web service APIs (with a OAuth consumer key plus secret.)¹⁸

Brokered authentication does not require the client and service to share a direct trust relationship. Instead, a broker authenticates the client and then issues a security token that the service can use to authenticate the client. The security token is always verified, but typically, the service does not

¹⁸ Technically OAuth is a specification for *authorization* and not *authentication*. Key Bridge web service APIs generally use "2-legged" OAuth for automated, machine-to-machine and authorization. Counter-party authentication is strongly implied but not guaranteed by user economic incentives to protect and secure their access credentials.

need to interact with the broker to perform the verification. This concept is shown in Illustration 51. PKI is a brokered security architecture.

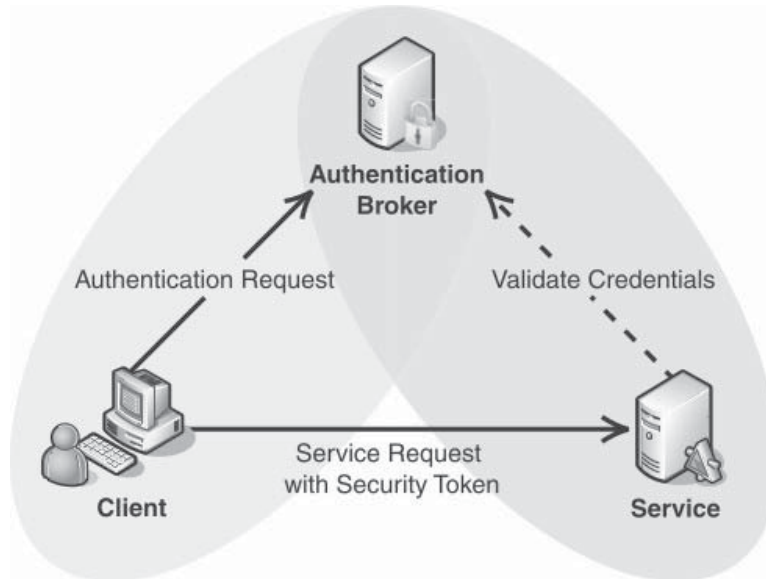


Illustration 50: Brokered authentication decouples the client and service.

SAS Infrastructure uses brokered authentication for most all counter-party authentication needs, including internal and external SAS to SAS peering, external SAS to ESC peering, User Access services, etc.

8.6 X.509 Digital Certificates

The X.509 specification defines a standard for managing public keys through a Public Key Infrastructure (PKI). Public keys are embedded and maintained in X.509 certificates, which themselves are digital (text) documents that bind a subject's identity to the embedded public key. The public key is from a public/private *asymmetric key* pair.

Identity information in a X.509 certificate is usually human readable, and may include a person's full name, e-mail address, title, etc. For machine to machine use, certificate identify information may alternatively include machine host names, processor serial numbers, media access control address (MAC Address), and other device-specific details. X.509 digital certificates contain several required and optional attributes that enable the identification of the subject. The following list of attributes are contained in an X.509 certificate:

- **Version number** is the certificate's X.509 standard version, i.e. 1, 2 or 3.
- **Serial number** is a unique identifier for the certificate.
- **Signature algorithm ID** is the algorithm used to create the digital signature.
- **Issuer name** contains the LDAP distinguished name of the certificate issuer.
- **Validity period** specifies the period during which the certificate is valid. This is declared with a effective and expiration date.
- **Subject name** contains the LDAP distinguished name of the subject represented by the certificate. The subject may be a person, organization, or application end point.
- **Subject public key** information provides the public key.
- **Issuer unique identifier** is the issuer identification.
- **Subject unique identifier** provides the identifier for the subject.
- **Extensions** that can be used to store additional information.
- **Signed hash** of the certificate data provides a hash of the preceding fields encrypted using the issuer's private key, which results in a digital signature.

X.509 certificates are endorsed and issued by a trusted third party, called a *certificate authority* (CA). In this context "endorsement" means that the identity information (i.e. the claims) within a X.509 certificate have been verified and may be trusted to be valid and true.

An example of a decoded X.509 certificate is shown in Text 1. The actual certificate is about one kB in size. It was issued as a self-signed certificate with validity between January 2016 and January 2026 by Key Bridge LLC, contains a 2048 bit RSA public key, and may be used for various cryptographic functions including Digital Signature, Non Repudiation, Data Encipherment, Key Agreement, CRL Signing, TLS Web Client Authentication and Time Stamping.

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 373680196295193711 (0x52f94289fc5f46f)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: O=Key Bridge LLC, OU=WSDB Registrar, CN=keybridgeglobal.com
    Validity
      Not Before: Jan 13 00:00:00 2016 GMT
      Not After : Jan 10 00:00:00 2026 GMT
    Subject: O=Key Bridge LLC, OU=WSDB Registrar, CN=keybridgeglobal.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:a8:73:be:49:fc:e0:79:4d:de:95:92:b1:c2:22:
        ...
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:FALSE
      X509v3 Key Usage: critical
        Digital Signature, Non Repudiation, Data Encipherment, Key
        Agreement, CRL Sign
      X509v3 Extended Key Usage: critical
        TLS Web Client Authentication, Time Stamping
    ....

```

Text 1: Sample X.509 certificate.

Custom security implementations that use X.509 certificates may depend on custom extensions that are not widely used or understood. These custom extensions must be included in the certificate by the certificate issuer when the certificate is created. Not all CAs may be willing or capable of adding custom extensions to certificates.

The validity period of an X.509 certificate tends to be much longer than that of other types of security tokens. For example, passwords are normally changed at shorter intervals, such as every 30 days. For this reason, it is critical to be aware of any possible compromise of an X.509 certificate private key, because it will be useful to an attacker for a considerably longer time than the secret key used in other security token types that have a much shorter lifespan.

8.6.1 Public Key Encryption

Public key encryption, also known as *asymmetric encryption*, is based on a public/private key pair. The public and private keys are mathematically linked such that any data that is encrypted with the public key can only be decrypted with the corresponding private key. This concept is shown in Illustration 52.

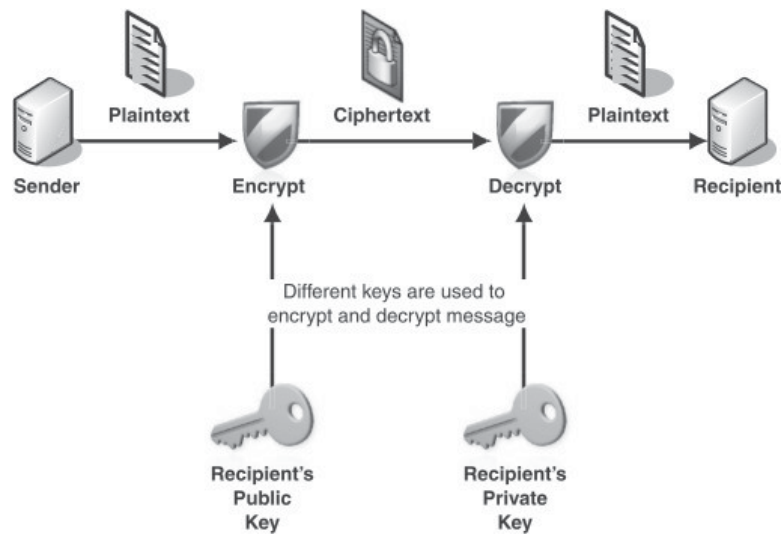


Illustration 51: Public key encryption and decryption

X.509 certificates use public key encryption (as compared with shared symmetric keys).

8.6.2 X.509 Digital Signatures

X.509 public keys may also be used to verify *digital signatures* created by a message sender.

A digital signature is produced by a message sender to bind message data to the sender's identity. This binding is implemented with the sender private key, which is used to create a digital signature of the data. The sender's corresponding public key, shared within the sender's X.509 certificate, may then be used to verify the signature by comparing the digital signature with the sender's public key and the received data. This concept is shown in Illustration 53.

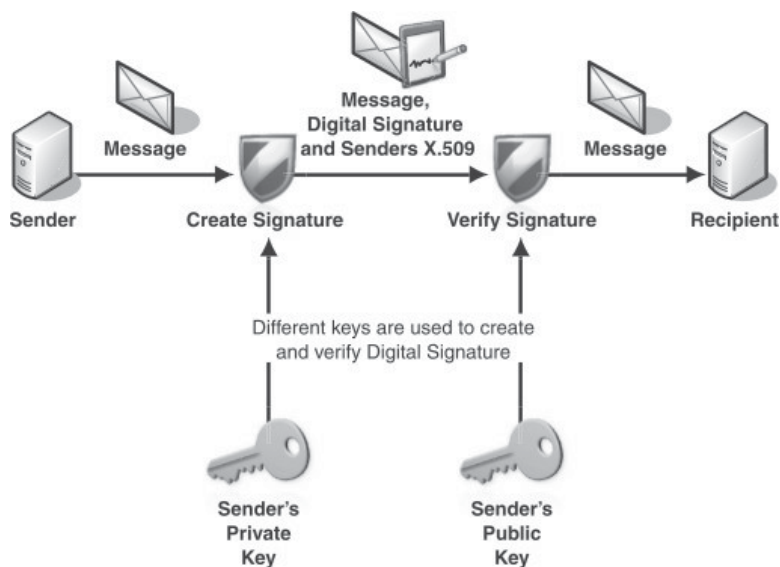


Illustration 52: Creation and verification of a digital signature

By this method a digital signature can assure a recipient that the message actually originated from the identified sender and that the message contents have not been altered in transit by a third party.

Because digital signatures rely on PKI, the sender's public key can be distributed openly to any receiving party while the private key is carefully guarded by its owner. A message recipient also need not have a trust relationship with the sender, but may instead rely on the CA-issued X.509 certificate (and its embedded public key).

Digital signatures are an important enabling technology for *message protection*, which is used extensively throughout the SAS Infrastructure.

8.7 Message Protection

SAS and CBSD end points send and receive plain text messages using standard Internet protocols (such as HTTP/HTTPS, REST, SOAP, etc.). Plain text messages are easily intercepted while in transit and may be viewed or potentially modified for malicious purposes. Such “man-in-the-middle” threats may be mitigated with appropriate use of message protection strategies. Message protection includes three main functions:

- **Data confidentiality** is the encrypting of message data so that unauthorized entities cannot view the contents of the message.
- **Data origin authentication** is the ability to identify and validate the origin of a message.
- **Data integrity** is the verification that a message has not changed in transit.

There are two main families of message protection implementation:

- **Transport Layer Security** where security features are implemented in the end-user's operating system, network or application and not in the exchanged messages.
- **Message Layer Security** where security features are implemented in the application and encapsulated in the exchanged messages.

SAS Infrastructure protects message data against threats such as eavesdropping and data tampering. Key Bridge SAS Infrastructure implements all three message protection functions and applies both types of protection (transport and message layer) according to the security demands of the specific application and context.

8.7.1 Data Confidentiality

SAS Nodes use asymmetric cryptography (also known as public key cryptography), to protect sensitive message data. When using asymmetric encryption the information is encrypted prior to transmission by a SAS Node. In this model the SAS Nodes encrypt data with the recipient's public key prior to transmission and the recipient uses its own private key to decrypt the data.

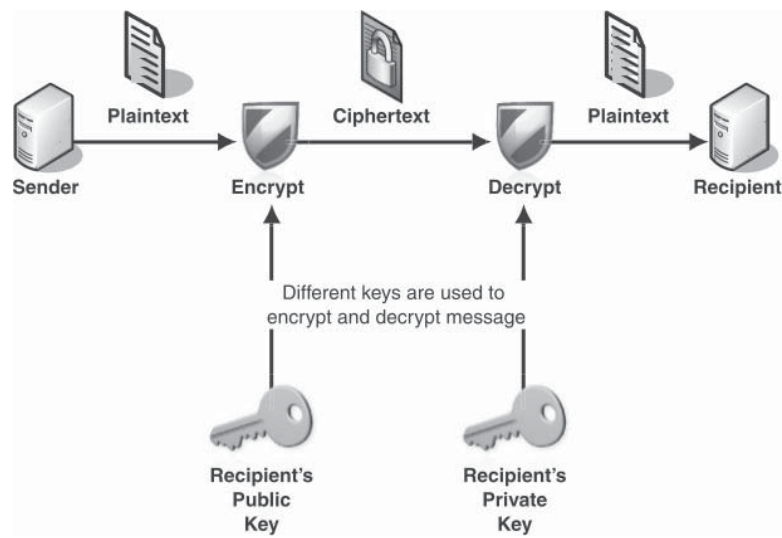


Illustration 53: The process of asymmetric encryption

The process of a asymmetric encryption is shown in Illustration 54 and involves the following steps:

1. The sender encrypts a plain text message with an asymmetric encryption algorithm and the recipient's public key. This creates an encrypted cipher text message.
2. The sender sends the cipher text message to recipient.
3. The recipient decrypts the cipher text message back to plain text using its private key.

8.7.2 Data Origin Authentication

Data exchanged between a SAS Node and a particular CBSD may pass through one or more intermediaries, including third party Internet hosts, etc. There is a risk that an attacker could manipulate messages in transit, which in the context of SAS and CBSD operation could maliciously alter the behavior of either party. Such message manipulation could take the form of data modification, or event substitution of credentials, to change the apparent source of the request message. These risks are mitigated through the application of *data origin authentication* and *non-repudiation* techniques.

SAS Infrastructure uses *asymmetric digital signatures* to implement data origin authentication and non-repudiation. A digital signature demonstrates the authenticity of a message or

documents, and a valid digital signature assures a message recipient that the message was created by a known sender.

In a SAS Node a asymmetric digital signature is created and processed with an public/private key pair unique to that SAS. The private key creates the signature and the public key verifies the signature. This concept is shown in Illustration 55.

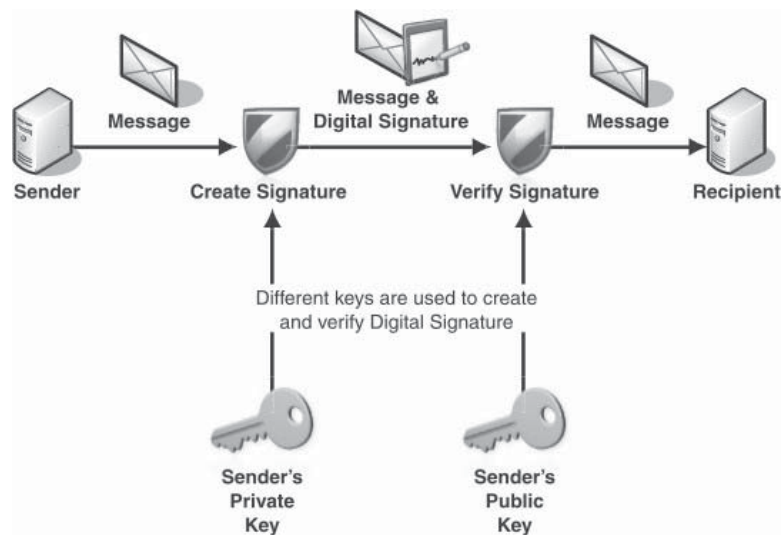


Illustration 54: Signing a message with an asymmetric signature.

The Digital Signature Algorithm (DSA) is most commonly used to create a digital signature.¹⁹ DSA involves the following steps:

1. The sender signs the message content using the sender's private key and attaches it to the message.
2. The sender sends the message and digital signature to the recipient.
3. The recipient verifies the digital signature using the sender's public key that corresponds to the private key that was used to sign the message.

8.7.3 Data Integrity

Data integrity is incorporated into all SAS Infrastructure message exchanges, primarily through the use of cryptographic message hashing and incorporation of cryptographic hash information into message digital signatures.

SAS Nodes implement data integrity using hash functions based on the Advanced Encryption Standard (AES) block cipher. AES is a symmetric-key algorithm used by the U.S. government since 2002 and used worldwide.

¹⁹ US Patent 5231668, Digital Signature Algorithm for technical details.

8.7.4 Transport Layer Security

Transport layer security is a strategy for protecting information exchange between two end points in a communications network. When using transport layer security the underlying operating system (or in certain circumstances the application) is responsible for security implementation. Examples of cryptographic protocols that implement transport layer security include Internet Protocol Security (IPsec), Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL).

It should be noted that the TLS *protocol* is just one (assertively named) implementation of several available transport layer security strategies.

Transport layer security is typically used in a client-server applications architecture, and an important characteristic is its implementation of and dependency on point-to-point (i.e. direct host-to-host) security.

For indirect communication transport layer security does not support data confidentiality, integrity or authentication. This concept is shown in Illustration 56, where a message must transmit through multiple points to reach its destination.



Illustration 55: Transport layer security is point-to-point.

In the illustrated example each intermediate host must resend the message over a separate secure transport layer connection. Using transport layer security alone the original message from the client is not cryptographically protected while in transit and may be intercepted and modified by each intermediary system.

SAS Infrastructure uses transport layer security for direct connections with remote hosts. Examples where transport layer security may be used include directly SAS to SAS peering links, SAS to ESC peering links and (possibly) SAS to CBSD communications where a domain proxy is not employed. SAS Nodes do not rely upon transport layer security alone however for any processes where an intermediary may have access to message data and where cryptographic protection is needed, in which case *message layer security* is used.

8.7.5 Message Layer Security

Message layer security incorporates and encapsulates cryptographic protection in to the message itself and has no dependency on underlying and intermediate systems. When using message layer security a message may be routed between a sender and recipient over any number of intermediate hosts and relays with no loss of cryptographic integrity or assurance. This concept is shown in Illustration 59.



Illustration 56: Message layer security is end-to-end.

Securing information using message layer security has several advantages over transport layer security, including:

- **Flexibility.** Using message layer security parts of the message, instead of the entire message, may be signed or encrypted. By this method intermediaries can view, process and modify parts of the message intended for them. An example of this is a message router (i.e. a SAS domain proxy) able to inspect unencrypted parts of the message to determine where to send the message, while other parts of the message remain encrypted for the intended end user.
- **Auditing.** Intermediaries such message routers, proxies, brokers and relays and can add their own headers to the message and sign them for the purpose of audit logging.
- **Multiple protocols.** Messages are not dependent upon any particular network protocol and secure messages may be sent over many different transport methods, such as Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Transmission Control Protocol (TCP) without having to rely on any specific protocol for security.

Message layer security is implemented in the application, and can be more complex than transport layer security, which is typically implemented in the operating system. Also, because each message is individually processed, message layer security requires more computational resources than transport layer solutions. For these reasons Key Bridge SAS Infrastructure uses message layer security in circumstances where information delivered to an end point must transit a intermediate system, but generally not where direct transport layer (i.e. point-to-point) connection is sufficient. Examples include SAS to CBSD communications that are aggregated via a domain proxy, ESC to SAS Node direct messaging, etc.

9 Key Bridge SAS Commercialization Strategies

Current rules entitle a SAS operator to charge CBRS users a reasonable fee for service. The 3.5 GHz ecosystem is emergent and still evolving rapidly, as are various underlying commercialization strategies for any fee recovery. Here we present current options for commercialization that Key Bridge may pursue and their concomitant fee collection processes.

Key Bridge understands and acknowledges the Commission's authority to review any fees that Key Bridge may establish for our commercial services and the Commission's authority to require changes to those fees if they are found to be unreasonable.

Note that the following descriptions are prospective and Key Bridge may pursue other commercial strategies, possibly to the exclusion of the strategies described here. Accordingly, KEY BRIDGE DOES NOT COMMIT AT THIS TIME TO ANY PARTICULAR COMMERCIAL STRATEGY, DEPLOYMENT, INVESTMENT, FEE STRUCTURES, MARKETING PLAN, ETC.

9.1 Services for General and Priority Access Users

Key Bridge expects to support GA services with the use of *Java Card* technology from our teaming partnership with Oracle. Java Card is a software technology that allows applications to run securely on smart cards. Java Card is widely used in SIM cards and ATM cards. Key Bridge expects to offer GA SIM cards direct to consumers via online retail and also indirectly through third-party retail channels and OEM vendors.

Key Bridge GA SIM cards with embedded Java Card technology from Oracle provide a cryptographically strong asymmetric key to bind a specific device with a responsible party. The Key Bridge GA SIM card will both authorize and authenticate the GA device to the Key Bridge SAS and also ensure the GA device validates and receives service exclusively from a FCC-authorized and certified SAS Infrastructure. A GA service SIM card package concept and demonstrator CBSD radio is shown in Error: Reference source not found.



Illustration 57: SIM cards enable secure, assured CBSD operation.

GA CBRS device registration and SIM card activation will be handled through a combination of automatic (machine-to-machine) data transfers and manual data entry by the user via a (to be developed) GA registration and enrollment web portal.

KEY BRIDGE EXPECTS TO SUPPORT PRIORITY ACCESS LICENSEE USERS THROUGH ENABLING SERVICES, CAPABILITIES AND RESOURCES FOR COMMERCIAL AND RETAIL NETWORK SERVICE PROVIDERS. KEY BRIDGE SAS INFRASTRUCTURE SHOULD BE INVISIBLE TO THE PA END USER AND FEES MAY BE ESTABLISHED BILATERALLY BETWEEN KEY BRIDGE AND EACH RESPECTIVE NETWORK SERVICE PROVIDER CUSTOMER. IN THE PAST SUCH ARRANGEMENT GENERALLY TAKE THE FORM OF FIXED OR VARIABLE-RATE FEE FOR SERVICE.

9.2 Automatic Frequency Planning (AFP)

Frequency planning in cellular networks is a difficult task; manual frequency plans are not scalable, are particularly difficult to optimize and prone to error. Efficient planning of large spectrum environments benefit from automatic frequency planning, and large dynamic spectrum environments as envisioned in the 3.5 GHz ecosystem will require high degrees of automation.

Automatic frequency planning is based on optimization of transmit and receive frequency assignment with knowledge of spectrum availability and empirically measured interference conditions. Key Bridge has experience offering these and other spectrum data services. We anticipate leveraging the described constellation of high-performance intelligent, network aware spectrum sensors and receivers.

Key Bridge automatic frequency planning (AFP) is a channel selection optimization technique. The Key Bridge AFP strategy for 3.5 GHz is based on an iterative frequency packing strategy and optimizes transmit and receive channel allocations while considering potential interference conditions.

Automatic frequency planning is useful for all service types including LTE, WiMAX and others. Key Bridge 3.5 GHz AFP services will combine interference predictions and analysis from spectrum consumption models, path loss and signal propagation predictions. Key Bridge intends to include empirical measurement data from ESC Infrastructure in our AFP algorithms.

9.3 Spectrum Mapping and Visualization

Key Bridge expects to include in our SAS Community Portal various spectrum mapping technologies that users may exploit for rapid, detailed visual inspection of CBSD spectrum environments. Key Bridge already provides spectrum mapping services and capabilities through our commercial API services, and we expect to make these services available to SAS users through existing web service and software developer kit to assist with network planning, device coexistence, and interference avoidance and mediation. An example spectrum coverage map is shown in Illustration 58.

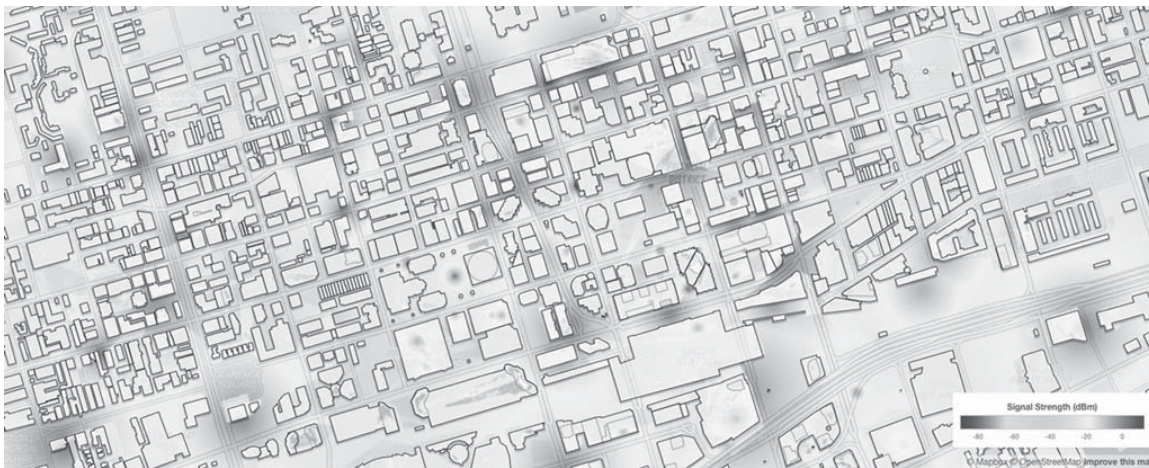


Illustration 58: Spectrum situational awareness is enhanced by empirical measurement.

The purpose of generating and using radio coverage maps is to better understand how a transmitter signal may propagate over a geographic region, or correspondingly what limitations on use a receiver may require across a geographic region. In this regard, radio mapping typically need not capture the fine nuances of different propagation model strategies, but instead focus on trending characteristics across an area of operation.

Key Bridge has experience incorporating spectrum sensor data with our spectrum mapping technologies to enable quick and detailed visual inspection of spectrum environments. This ability combines predicted coverage models with empirical measurement and presents a highly accurate digital representation of real-world spectrum environments.

Key Bridge expects to make available various spectrum mapping technologies that users may exploit for rapid, detailed visual inspection of CBSD spectrum environments and to integrate empirical measurements from the ESC into these mapping services.

9.4 Managed PKI Service

Key Bridge has partnered with Symantec to provide signed digital certificates and a robust, globally deployed public key infrastructure (PKI) suitable for authentication and encryption requirements for use across the 3.5 GHz ecosystem.

The Symantec PKI Service is a PKI certificate management and authentication service running proven, globally managed, highly reliable infrastructure and providing all essential security services needed for establishing trust in online electronic transactions that require confidentiality, integrity, identity authentication and non-repudiation.

- Real-time issuance to customers, business partners, Web services applications and network devices
- Full life cycle management to issue, renew, revoke, and manage digital certificates with maximum flexibility
- Automated enrollment for users, servers, applications, network devices
- Standards-based digital certificates can be installed on open standards authentication devices with native PKI support: computers, tokens, smart cards, mobile phones, and more
- Validation of certificates through the highly available, secure infrastructure with daily updated Certificate Revocation Lists (CRLs)
- Audited policies and procedures to meet the most rigorous compliance requirements

Advantages of the Key Bridge embedded certificate and PKI solution, powered by Symantec, include:

- The longest running commercial PKI platform in the world
- More than 150 million device certificates issued to date
- 42,000 Class 1 certificates and more than 16,000 ECA certificates issued each year
- 15,000 secure online transactions enabled every second

9.5 Embedded Device Certificates

Digital certificates embedded into hardware devices enable service providers to authenticate remote devices before allowing access to networks and services. Device Certificates are a high-volume, high-performance batch issuance certificate service that provides a fast, efficient, and cost-effective way to embed X.509 certificates into any type of hardware device during the manufacturing process. The X.509 certificate allows service providers to perform strong authentication of distributed hardware and prevent unauthorized or cloned devices from obtaining access.

How Device Certificate Issuance Works

1. Device manufacturers order certificates in bulk from a list of MAC addresses, unique device IDs for the certificates or by providing a standard PKCS10 Certificate Signing Request.
2. Device manufacturer receives issued certificates and private keys, if requested, in an encrypted format.
3. Device manufacturer embeds the certificates during the device manufacturing process.

Key Bridge and Symantec will offer a turnkey solution to generate batches of digital certificates and private keys through an easy-to-use Web interface. The digital certificates will authenticate certified 3.5 GHz devices to the Key Bridge SAS and also ensure the device validates and receives service exclusively from a FCC-authorized and certified SAS Infrastructure.

A useful example from the WiMAX™ Industry

Symantec presently supports the WiMAX Forum® requirements for strong mutual authentication of devices and authentication servers using X.509-standard digital certificates.

The WiMAX Forum selected Symantec as the sole provider for its Server PKI for service providers. Symantec was also chosen to provide X.509 PKI certificates to WiMAX Device Manufacturers.

10 Appendix: Femto Access Point Use Case

The CPE WAN Management Protocol (CWMP), managed and published by the Broadband Forum, defines a mechanism that encompasses secure auto-configuration of a customer premises equipment (CPE), and also incorporates other CPE management functions into a common framework.²⁰

CWMP is enabled by a auto-configuration server (ACS); a component in the broadband network responsible for auto-configuration of the CPE for advanced services. The CWMP protocol allows an ACS to provision a CPE or collection of CPE based on a variety of criteria. The provisioning mechanism includes specific provisioning parameters and a general mechanism for adding vendor-specific provisioning capabilities as needed.

Key Bridge is working to support *Femto Access Point* (FAP, also called *femtocell*) access and interoperability with SAS Nodes using existing the CWMP standards and protocols. FAP management generally requires a fundamentally different management approach from the traditional cellular infrastructure network elements, and Key Bridge SAS Node integration of TR-069 CPE WAN management standards naturally meets this requirement with a remote management protocol specifically designed for consumer CPE devices. For context, a full complement of device and service managed standards is shown in Illustration 60. In the illustrated example the Key Bridge SAS Node provides the function of *Auto-Configuration Server*.

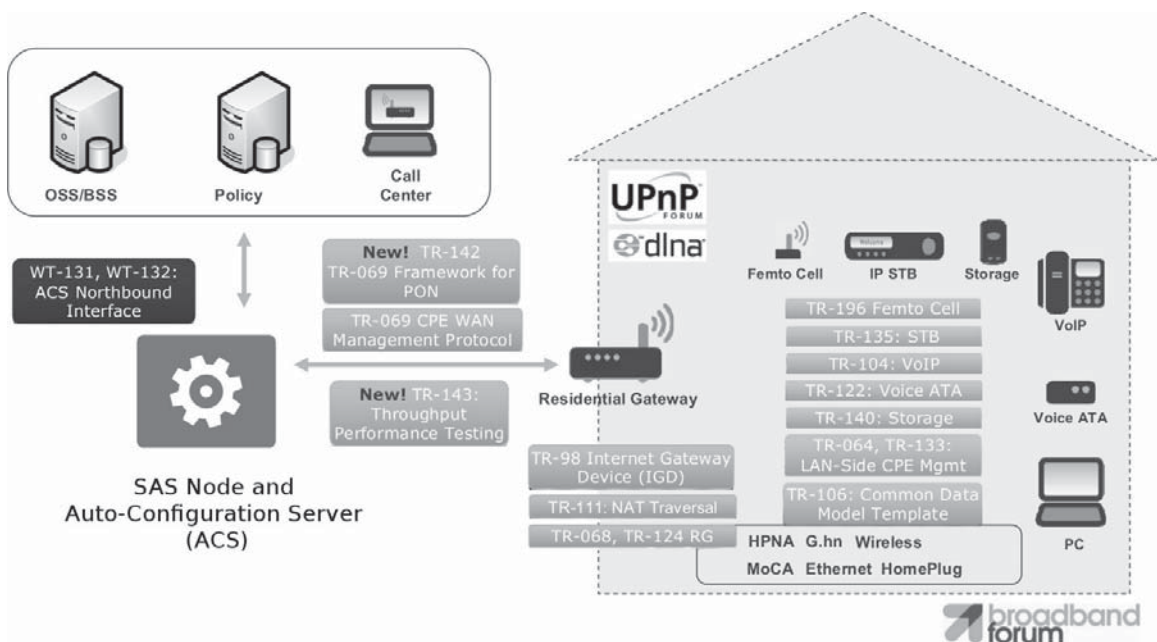


Illustration 59: Key Bridge SAS Node is a Auto-Configuration Server

²⁰ The Broadband Forum at <http://www.broadband-forum.org>

There are several main characteristics that separate a FAP from the traditional cellular network infrastructure. A FAP is a consumer CPE device located at the end-user's premise with intended coverage and the capacity orders of magnitude smaller than a traditional macrocell. FAPs are expected to use the existing fixed broadband technology, such as cable or xDSL, as the backhaul to a mobile network, with the number of FAP devices deployed and to be managed orders of magnitude higher than a traditional macrocell based system.

The physical control of the FAP device itself is outside the control of the mobile operator that provides the service. This includes, for example, the physical state and condition of the device plus the location of the device where it may be installed and operated.

Since the number of devices to manage is order of magnitude higher than the traditional macrocells, a different approach of device management may be required. The CWMP protocol provides flexible support for various business models for distributing and managing CPE, including CPE provided and managed by a network provider; pre-registered CPE purchased in retail, such as a mobile-phone like model; and CPE purchased in retail with a post-installation user registration process.

The CWMP protocol supports a flexible connectivity model, where both CPE and ACS may initiate a connection. This is an important scaling capability, and avoids the need for persistent connections to be maintained between each CPE and an ACS. The functional interactions between the ACS and CPE are also independent of which end initiated the establishment of the connection. For example, in circumstances where ACS initiated connectivity is not supported all ACS transactions are still possible over a connection initiated by the CPE.

10.1 Key Bridge FAP Services

The Key Bridge FAP services implement all data exchange transactions identified in Part 96 and presently under development in a multi-stakeholder group, but translated to work according to the CWMP protocol and associated data models. In this regard the Key Bridge SAS FAP management capability parallels the new SAS to CBSD protocols presently under development through a multi-stakeholder group in which Key Bridge is a participating member while also seeking to establishing backwards compatibility with existing, mature and well established standards for device management.

A example network configuration showing how various FAP devices may be supported by a Key Bridge SAS Node is shown in Illustration 61, where the SAS Node implements and incorporates Part 96 transactions into its ACS functionality.

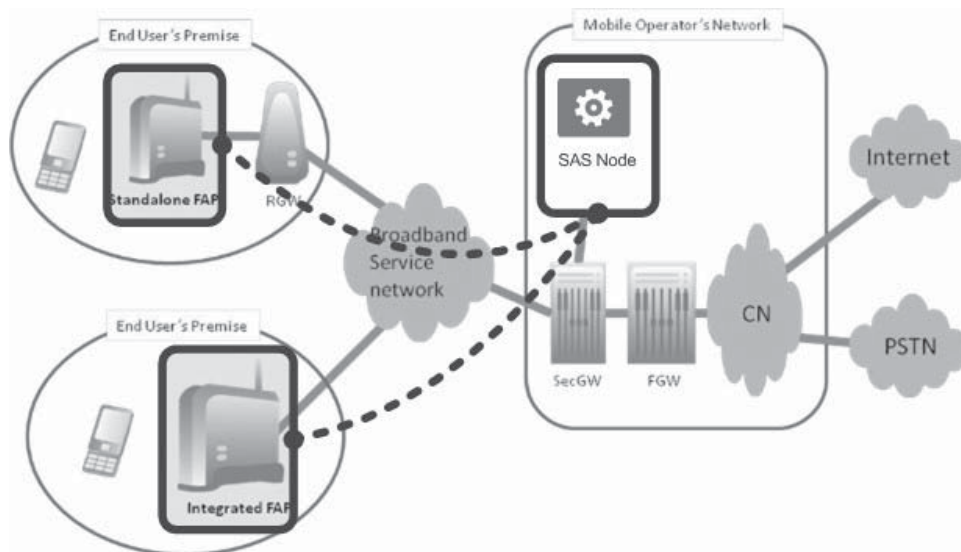


Illustration 60: Key Bridge SAS Nodes support TR-069+196 clients.

The TR-069 and TR-196 standards (among others) for configuring and managing Femto Access Points are mature and well established standards for device management, with TR-069 widely used throughout the broadband service delivery ecosystem to manage tens of millions of CPE devices including cable modems, xDSL modems, set top boxes, SIP phones and gateways, and more. Key Bridge SAS Node implementation and extension of the CWMP protocols provide a simpler and smoother FCAPS implementation for operators by reusing technology that is already proven in present mass CPE deployments, a established and well-known standards-based technology platform for the vendor community, and simple and error-free “plug-and- play” installation for end users.

11 Appendix: SSRF Interference Incident Report

Interference Incident Reporting enables standardized reporting significant interference, rapid identification of potential sources, and resolution assistance.²¹

Standard Spectrum Resource Format (SSRF) is a standardized data format for exchanging spectrum management-related data. While the original scope of use for SSRF is within the Department of Defense (DOD) many of the business processes enabled by SSRF are also required for commercial spectrum management and by national spectrum regulators and administrators as they introduce dynamic spectrum sharing rules and regulations.

SSRF is a component technology supporting a number of DOD spectrum operations and systems shown in Illustration 62. These include GEMSIS, Coalition Joint Spectrum Management Planning Tool (CJSMP), Spectrum XXIO, Stepstone and others.

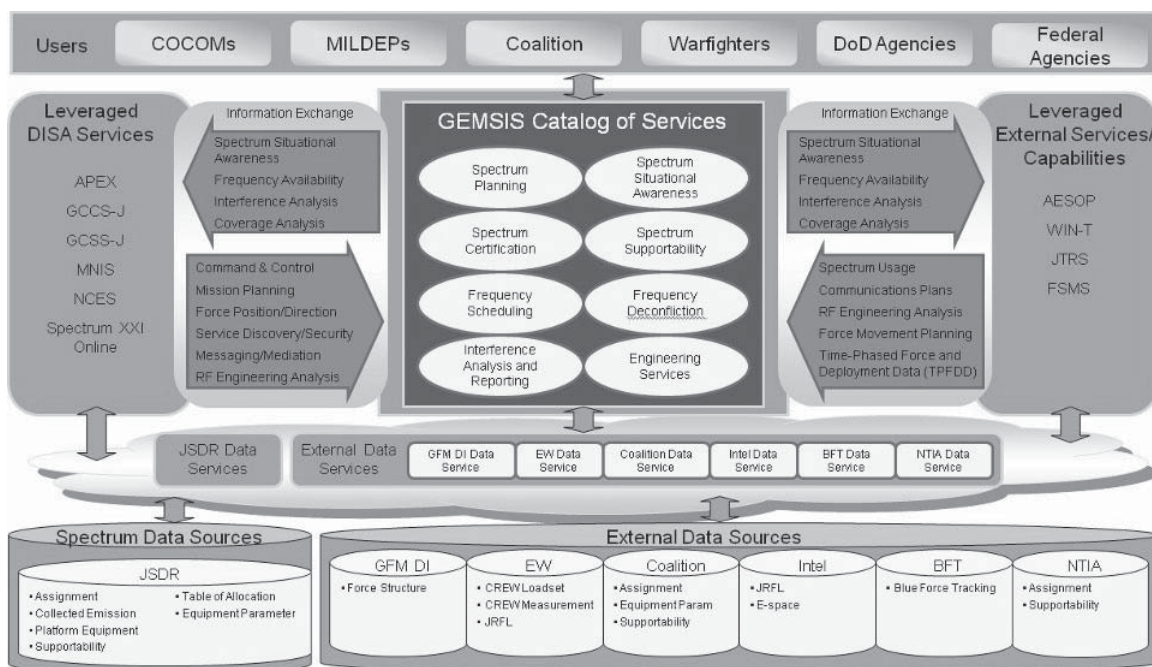


Illustration 61: SSRF is an essential technology for many DoD spectrum systems.

Common goals for these various systems are enabled by SSRF and include:

- Transform spectrum operations to a responsive and agile capability to request, assign, allocate, and deconflict portions of the electromagnetic spectrum
- End-to-end spectrum supportability frequency assignment
- Software definable radio waveform spectrum management support

²¹ This appendix is excerpted from the OpenSSRF portal at <http://openssrf.org>

- Strategic spectrum management planning
- Modeling and simulation for mission planning, rehearsal, and acquisition
- Increased common picture of spectrum situational awareness of friendly and hostile forces

The Standard Spectrum Resource Format (SSRF) defines standard data elements for automated exchange of radio-frequency (RF) spectrum-related data. SSRF is managed under the authority of DOD Directive 5100.35, Military Command, Control, Communications, and Computers Executive Board (MC4EB) and published in the MC4EB Pub 8 document. The SSRF specification is published and placed in to the public domain by the MC4EB. The SSRF specification is royalty-free and license-free.

OpenSSRF is a open source, royalty-free, license-free reference software implementation of the most recent SSRF specification; currently v3.1.0. The OpenSSRF software code is licensed under the Apache License, Version 2.0.

OpenSSRF is developed and maintained by Key Bridge LLC in collaboration with members of the The Wireless Innovation Forum Spectrum Innovation Committee and with unofficial advisory support from the Defense Spectrum Organization. More information is available at <http://openssrf.org>.

Introduction to SSRF Interference Incident Reporting

To provide full spectrum management capability it is important that all significant interference is reported. All interference has a source (the equipment causing the interference) and a victim (the system or assignment suffering from the interference), and resolving interference between the two may be achieved by either readjusting the source or victim parameters and configuration.

Since it is important to avoid causing further interference effects on other systems while trying to resolve a particular interference case the resolution process should be based on careful analysis of the relevant EM environment. Therefore the process should normally involve the use of appropriate spectrum analysis tools.

Typically, interference will be resolved at the lowest possible organizational level. This however, is not always the case, therefore the interference reports must be generated and forwarded through the spectrum management organizational hierarchy.

Assuming the victim of the interference is unable to resolve the interference, interference reports should be created at the victim site and sent to higher headquarters [IAW CJCSI 3320.02].

The lowest level receiving the interference report will attempt deconfliction using the tools available at that level (database, analysis tools applying various propagation and terrain models, etc). If the interference cannot be resolved at the point where the interference is initially detected, an interference report will be prepared and forwarded to the next level for action. In cases involving international coordination, the interference report may be forwarded to the relevant national authority.

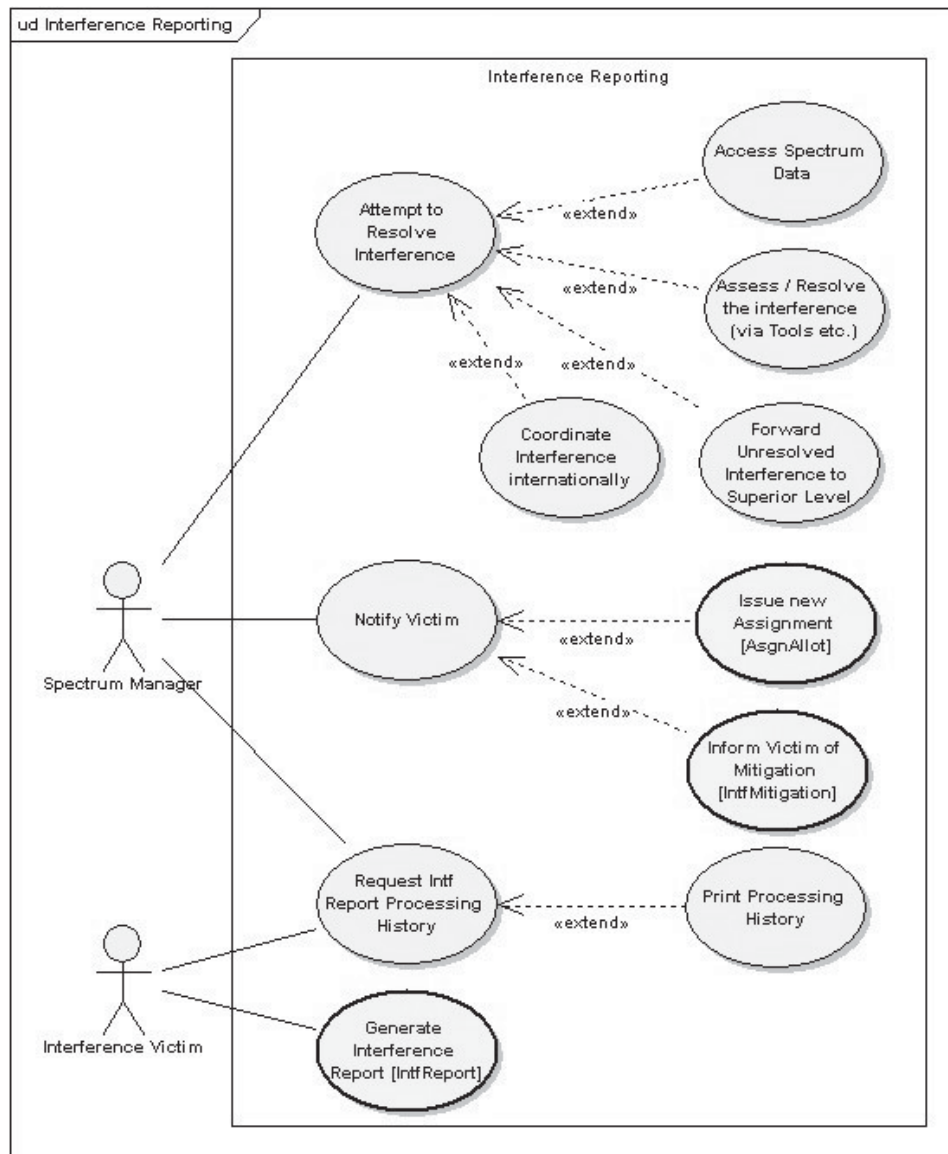


Illustration 62: Use Case Diagram for Interference Reporting.

Regardless of level at which an interference issue is resolved and the report closed the final report should be forwarded to the central database for historical reference.

Interference Incident Report Processing History

The interference resolution process may result in an interference report being forwarded through the spectrum management organizational hierarchy. As the interference report is processed through the organization, the status changes and the actions taken at each processing stage shall be recorded and made available to the requesters. A processing history of the interference and its

mitigation is recorded for later reference.

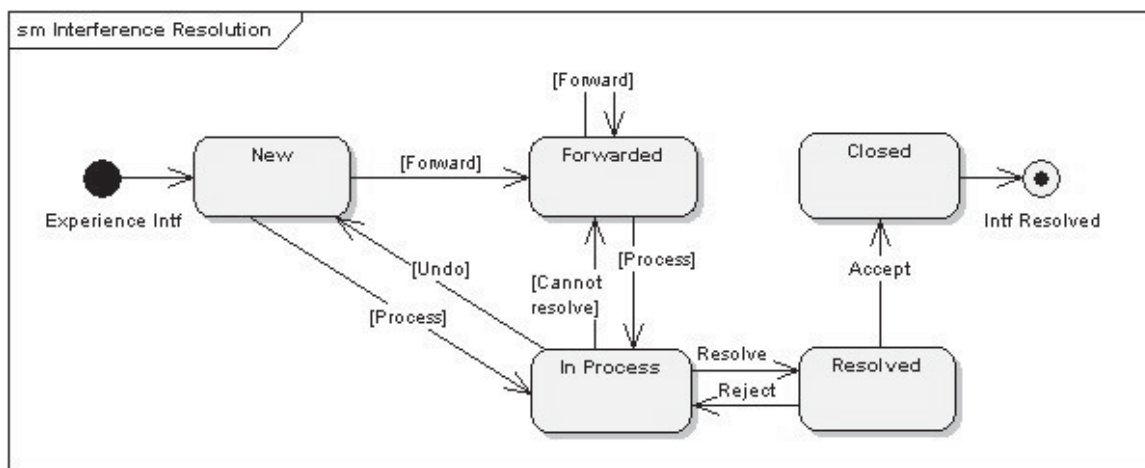


Illustration 63: Interference incident processing history.

A state transitions of an interference report concept is shown in Illustration 64 above while it travels through the organizational hierarchy during a resolution process. According to this state diagram, a message is in a New state when it is first created and sent to an immediate spectrum management authority.

- If the receiving authority decides that the message can be processed (resolved) at his/her site, the message is put into the In Process state and a resolution is attempted.
- If the problem is handled the message is put into a Resolved state until the user accepts the resolution, moving it to a Closed state and terminating the process.
- If the user rejects the resolution, the message is sent back to the In Process state.
- If the first recipient can not handle the message, the message is forwarded to the next level of authority in the spectrum management organizational hierarchy. Therefore the message is put into a Forwarded state.

The forwarding process is repeated until the appropriate authority resolves the issue. An interference processing history will provide the sequence of these transitions.

Interference Incident Report Message and Data Fields

The processing history will accumulate in the Status element list under the main Interference Report (see *IntfReport* element). Requesting the processing history can be achieved by sending a Data Request (see Administrative Element) message containing the dataset reference of the requested *IntfReport* element.

The Interference Incident Report Data Object contains information on a source and victim of an interference incident. Field names, descriptions, data types and enumerated values are defined in

the SSRF specification. An Interference Incident Report also contains a POC reference to a Contact, Organization or Role. An example SSRF Interference report message is shown in Illustration 65.

```
<IntfReport serial="BEL:AR:IR:123" usageType="A" entry="2004-05-20" lastMod="2006-11-05T12:30:00Z">
  <... other Common elements ...>
  <Status state="ORIGINATED BY" dateTime="1995-12-31T15:33:48Z" byContact="BEL:AR:CN:UNIT1/123"/>
  <Remarks xpath="/Status[1]">Interference detected and cannot be resolved here.</Remarks>
  <Status state="FORWARDED TO" dateTime="1996-01-16T16:31:12Z"
    fromContact="BEL:AR:CN:UNIT1/123" toContact="BEL:AR:CN:COMBASE/129"/>
  <Remarks xpath="/Status[2]">This interference requires higher command involvement.</Remarks>
  <Status state="RECEIVED BY" dateTime="1996-01-17T16:31:12Z" byContact="BEL:AR:CN:COMBASE/129"/>
  <Remarks xpath="/Status[3]">Received an interference report.</Remarks>
  <Status state="IN PROCESS AT" dateTime="1996-02-01T09:12:12Z" byContact="BEL:AR:CN:COMBASE/129"/>
  <Remarks xpath="/Status[4]">We can resolve this interference here.</Remarks>
  <Status state="CLOSED BY" dateTime="1996-03-13T16:00:05Z" byContact="BEL:AR:CN:COMBASE/129"/>
  <Remarks xpath="/Status[5]">Interference resolved. The source system power was reduced.</Remarks>
  <... other Common + IntfReport elements...>
</IntfReport >
```

Illustration 64: Example interference report message data.

The resulting SSRF message reply to this request MUST contain the *IntfReport* element including the accumulated status elements to indicate the stages of the resolution process.

Additional information about the SSRF protocol, including detailed documentation and open source software, are available online without cost at <http://openssrf.org>.

12 Appendix: Joint Spectrum Interference Resolution

Joint Spectrum Interference Resolution (JSIR) is a process designed to mitigate or define the procedures to mitigate Electromagnetic interference (EMI) that regularly hampers the Command and Control (C2) of military/non-military operations by degrading essential systems that use the electromagnetic spectrum. Since EMI can be caused by enemy, neutral, friendly, or natural sources, it generally must be resolved on a case-by-case basis.²²

The intent of the JSIR procedures is to resolve EMI incidents at the lowest possible level within the command structure. However, when the cause and recipient of the interference are not within the same component force or supporting element, resolution may require assistance from the command, Combined Joint Task Force (CJTF), service spectrum management HQ or higher levels of authority.

The JSIR program was established in October 1992 by the DoD to address persistent and recurring EMI problems affecting DoD systems. The JSIR program replaced the DoD Beaconsing, Intrusion, Jamming, and Interference program that was disestablished on 30 June 1992.

The JSIR program focuses on EMI events and then provides an actionable means to alert the appropriate C/S/A on interference issues. The program is coordinated and managed for the Joint Staff Command, Control, Communications, and Computer (C4)/Cyber Directorate (J-6) by the JSC, Annapolis, Maryland. The program itself is centrally managed; however, the execution process is highly decentralized. Each of the DoD components shares responsibility for successful execution of the JSIR program (reference b).

The objective of the JSIR program is to detect, report, track, archive, analyze, and resolve EMI. The resolution process for EMI events includes:

- a) Detection, verification, characterization, and reporting.
- b) Geo-location, analysis, and identification.
- c) Resolution, includes development and implementation of corrective courses of action to regain use of the affected spectrum.
- d) Tracking the incident to closure, providing status updates, and archiving the incident for future reference.

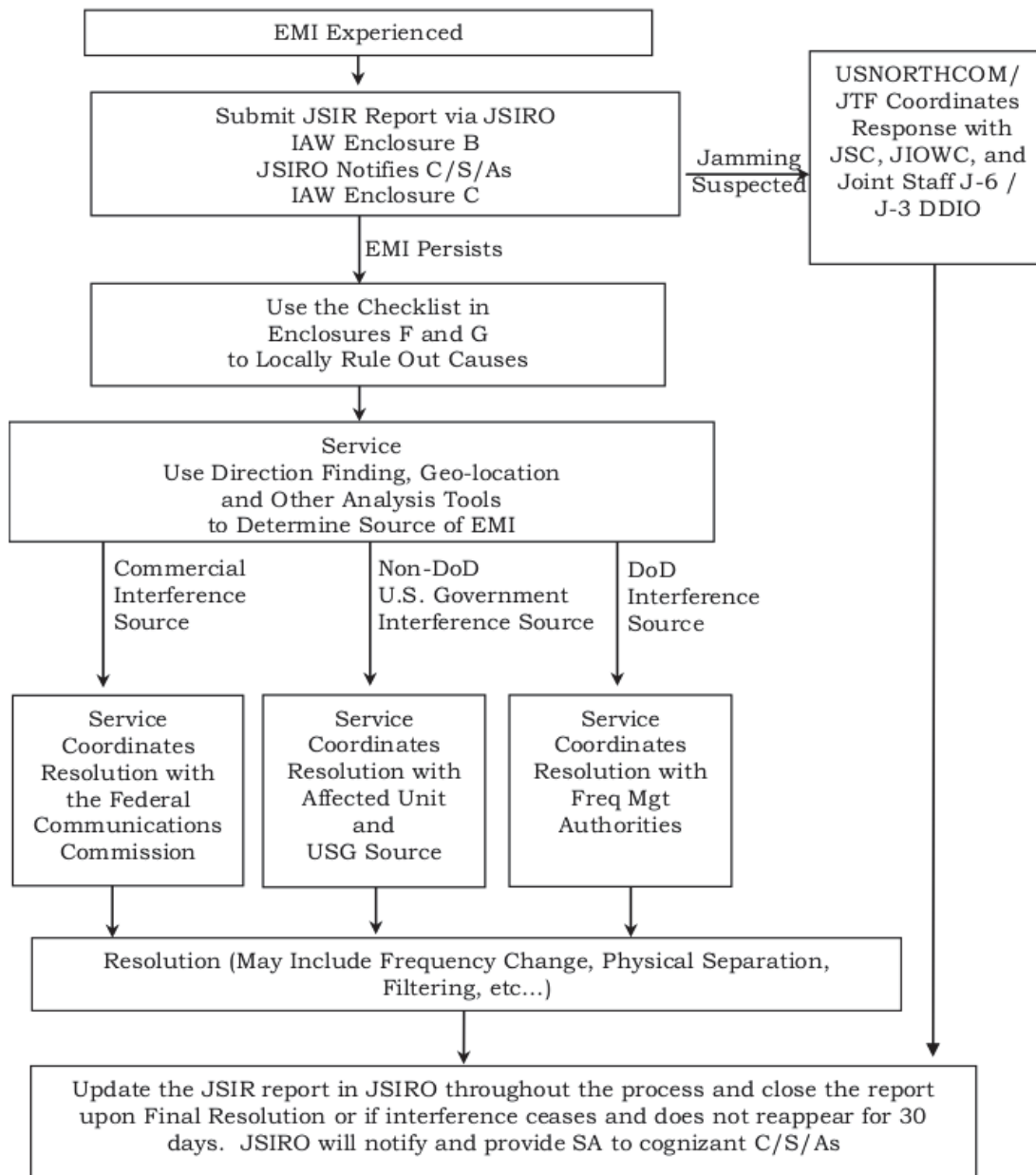
In cases of terrestrial interference within US&P, to include satellite downlink interference, the C/S/A owning or operating the affected system is responsible for investigating and resolving the interference. Downlink interference is defined as the part of the transmission link reaching from the satellite to the ground. ... Uplink interference is defined as the part of the transmission link from the earth station to the satellite.....

The JSIR detection and resolution processes for terrestrial and satellite interference are shown below.

²² This appendix is excerpted from the OpenSSRF portal at <http://openssrf.org>

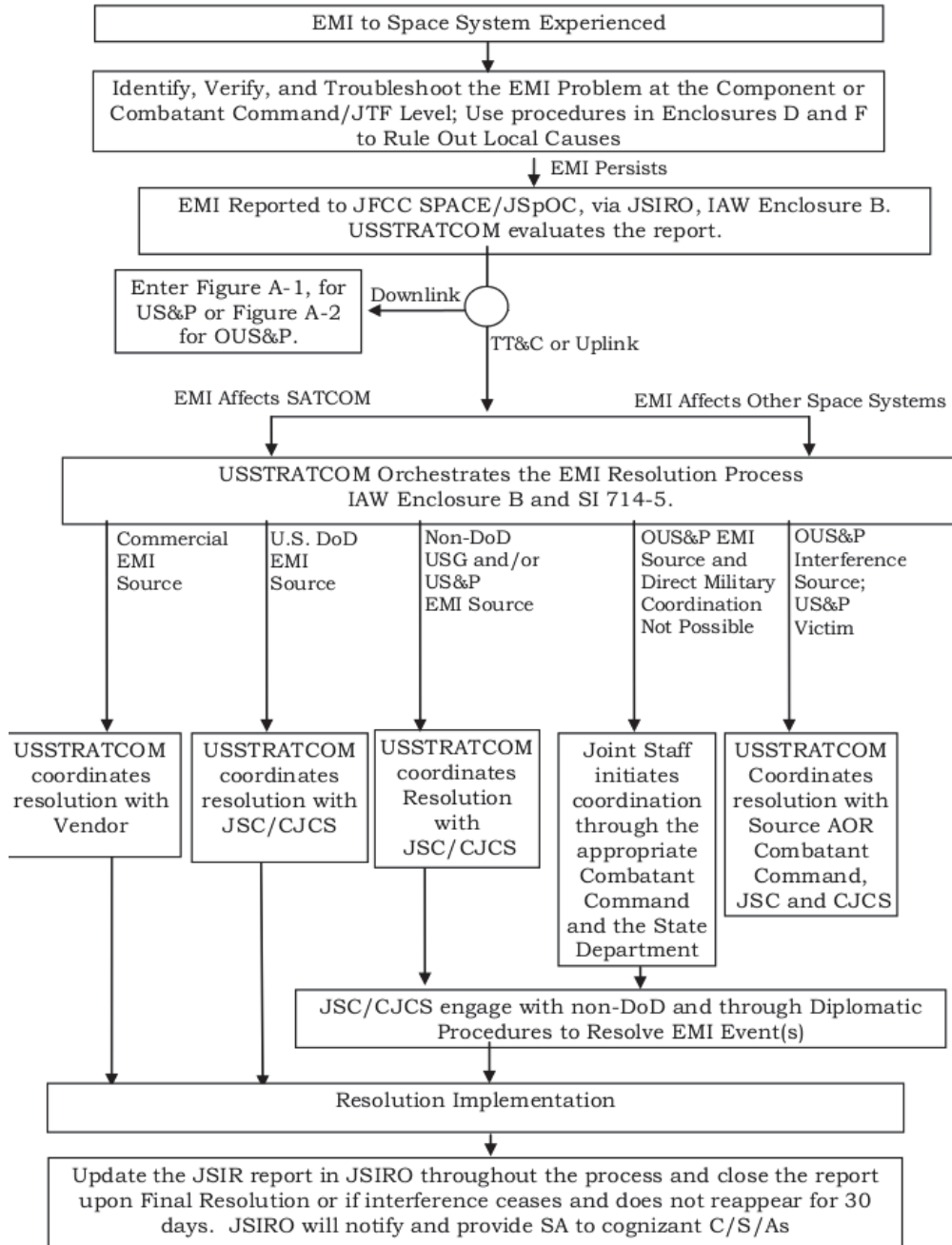
CJCSM 3320.02D

3 June 2013

US&P Terrestrial JSIR Process*Illustration 65: US&P Terrestrial JSIR Process.*

CJCSM 3320.02D

3 June 2013

Space System EMI Resolution Process*Illustration 66: Space System EMI Resolution Process*

Operating Clearance

Note that the Operating Clearance business process is not authorized for U.S. Forces but it may be used by some allied forces. It is described here for informational purposes.

The aim of the Operating Clearance process is to facilitate the timely provision of information leading to compatible systems that use the electromagnetic spectrum. It allows the operational spectrum managers to assess, with a certain degree of confidence, whether the equipment which will be brought into the operational theater will operate without creating interference. The Operating Clearance is the tactical version of the full Spectrum Supportability process; it **MUST NOT** be used as a replacement of the full Spectrum Supportability and **MUST** only be used in cases of short-term requirements in support of a critical operation. Acceptance of this abbreviated procedure is at the discretion of the commander.

A summary of the Operating Clearance process is illustrated below.

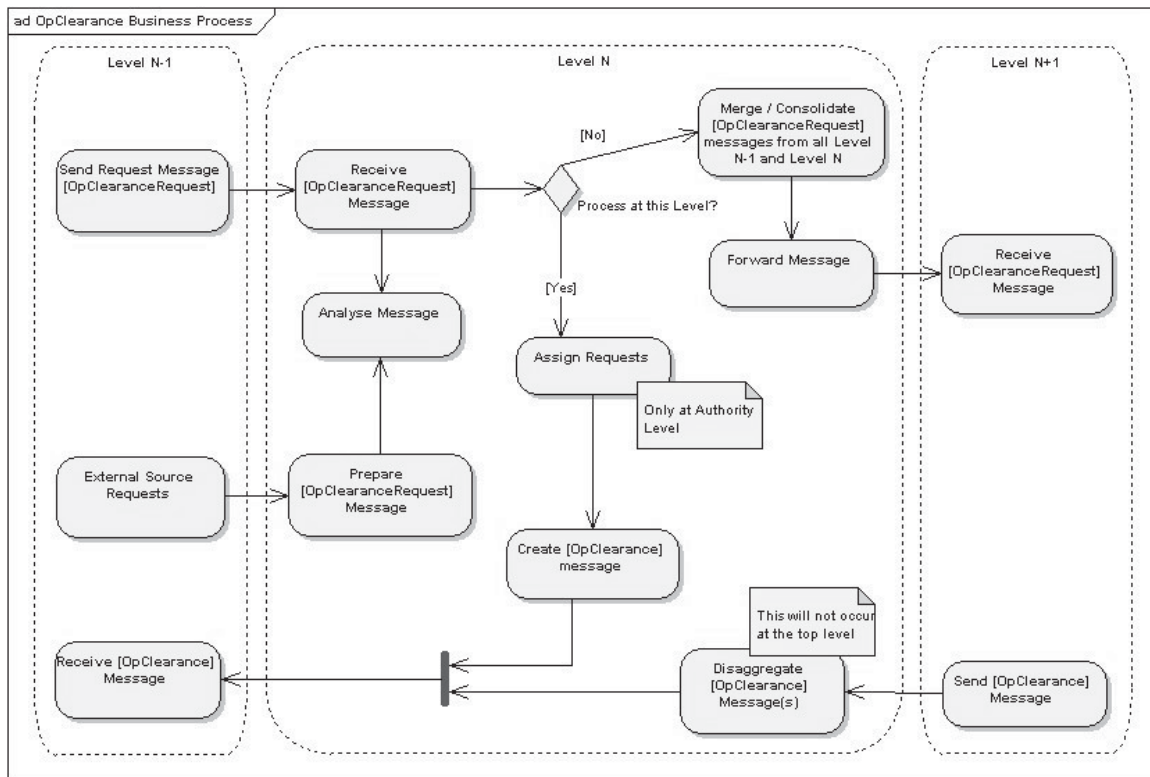


Illustration 67: Operating Clearance business process.

The activity diagram for Operating Clearance process is shown below.

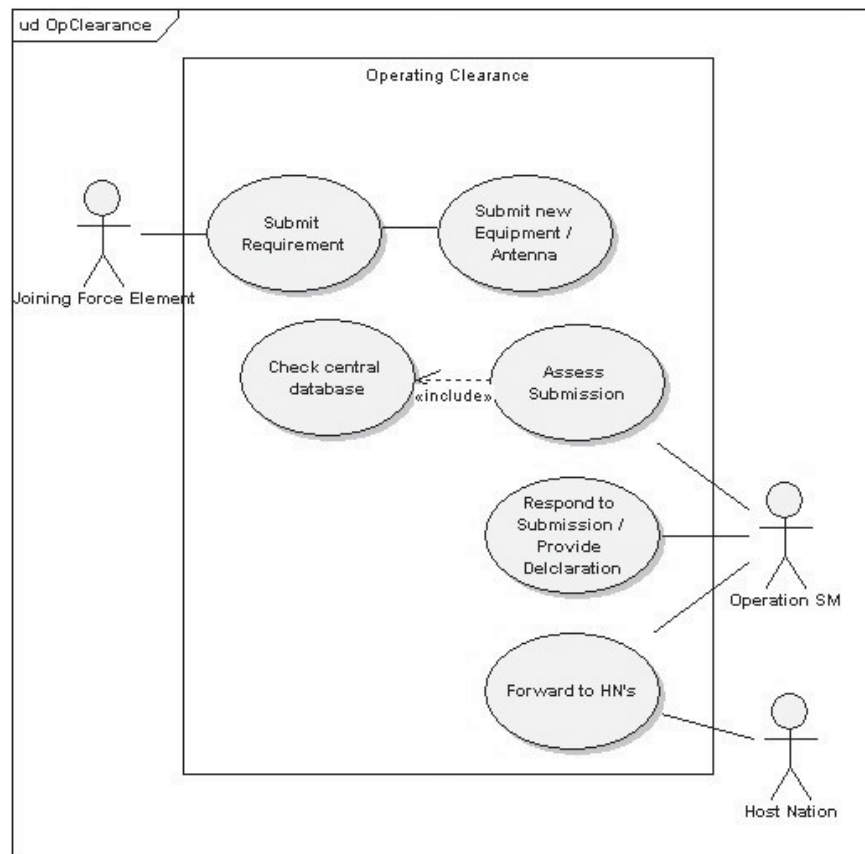


Illustration 68: Operating Clearance activity diagram.